THE MIRAGE OF USE RESTRICTIONS*

RIC SIMMONS**

The Fourth Amendment strikes a balance between Americans' privacy interests and the government's need to investigate crime. It does so almost exclusively by placing restrictions on how the government collects information: if the government surveillance constitutes a "search," the government must meet certain legal standards before it can engage in that surveillance. Over the past few decades, technological advances have exponentially increased the government's ability to collect information and many of these new surveillance methods do not fit into the traditional definitions of a Fourth Amendment search. In response, courts and commentators have searched for new doctrines to define and limit the government's surveillance power. One of the more popular proposals that has been advanced is to force the government to adopt "use restrictions"—limitations on what the government can do with information that it collects or that is already in its possession. This new type of restriction represents a significant shift from the current paradigm of regulating government surveillance: a shift away from regulating how information is collected and towards regulating how the information is used.

Use restrictions on surveillance data have been termed the "future of surveillance law." They have been proposed in many different contexts, such as restricting how the government can process massive amounts of public data; limiting the use of information from DNA databases; regulating the information obtained through special needs searches; restricting the use of information that law enforcement obtains after conducting a search of a computer; or limiting the use of data from drones or police body cameras.

This Article concludes that most types of use restrictions do not have sufficient legal justifications. It first reviews the many

* © 2017 Ric Simmons.

** Chief Justice Thomas J. Moyer Professor for the Administration of Justice and Rule of Law, Moritz College of Law, The Ohio State University. I would like to thank Angela Lloyd, Michael J.Z. Mannheimer, Matt Tokson, Craig Konnoth, and the participants of the 2016 CrimFest Conference for their terrifice feedback. I would also like to thank Tresha Patel for her excellent research assistance.

possible applications of use restrictions and discusses five potential doctrinal bases to justify them: (1) apply an "ongoing seizure" doctrine; (2) create a purpose test for the exclusionary rule; (3) re-define a "search" as including the processing of information, not just its collection; (4) make the purpose of the data collection a factor in determining whether collecting the data is a search; and (5) limit which government agencies are allowed access to the data that is collected. This Article then demonstrates that most use restrictions cannot be justified by any of these doctrinal bases. This Article further argues that adopting use restrictions would be bad policy, since adopting restrictions would discourage the creation of tighter collection restrictions, give the government possession of vast amounts of our private data, and in some cases unduly hinder legitimate law enforcement functions. Therefore, this Article opposes the movement towards use restrictions and proposes that courts and legislatures maintain the focus of Fourth Amendment law on collection restrictions and move forward with use restrictions only in very limited circumstances.

INTRODUCTION

Fourth Amendment law has undergone numerous dramatic changes over the past fifty years. In 1967, the Supreme Court decided *Katz v. United States*,[1] shifting the Fourth Amendment focus from property rights to privacy rights.[2] Over the next few years the Court would continue to make radical changes in this area of law: it created an entirely new category of seizures and searches that do not require a warrant or probable cause,[3] approved a wide variety of widespread, suspicionless searches as long as they were conducted for a non-law enforcement purpose,[4] permitted searches of arrestees even if there was no chance of finding contraband or weapons,[5] and allowed the police free access to any information that a suspect shares with a third party.[6]

Even though each of these cases represented radical changes in Fourth Amendment law, they all shared the same fundamental assumption that has formed the basis of nearly all Fourth Amendment jurisprudence since the founding of our country: these cases all focused on the *collection* of the information as the basis for

1. 398 U.S. 347 (1967).
2. *Id.* at 353.
3. Terry v. Ohio, 392 U.S. 1, 30–31 (1968) (holding that a law enforcement officer may stop and conduct a limited search of a person if the officer "observes unusual conduct," reasonably concludes that criminal activity is underway and that the involved persons may be armed, and identifies himself as a law enforcement officer and makes reasonable inquiries).
4. *See, e.g.*, Camara v. Mun. Court, 387 U.S. 523, 538–39 (1967) (allowing building inspectors to obtain a warrant for a search using a decreased showing of probable cause); *see also* New Jersey v. T.L.O, 469 U.S. 325, 345–46 (1985) (allowing a school to search a student's purse without a warrant or probable cause).
5. United States v. Robinson, 414 U.S. 218, 218 (1973) (stating that custodial arrest allows for a full search of the person without a warrant).
6. Smith v. Maryland, 442 U.S. 735, 745 (1979).

deciding whether the Fourth Amendment was violated.[7] Recently, however, a truly revolutionary idea has begun to gain traction among Fourth Amendment scholars and some courts: evaluating the government action based on how the government *uses* the information rather than how the government *obtained* the information.

Use restrictions on government surveillance have been called the "future of surveillance."[8] They have been hailed as an ingenious solution to the twenty-first century's most vexing Fourth Amendment problems.[9] New surveillance technologies such as drones and police body cameras have provided police with unprecedented amounts of data about our activities; use restrictions are seen as a way to ensure that the police do not abuse this data.[10] Police can use new methods of information processing, popularly known as "big data," to gain insight into our private lives using seemingly innocuous bits of publically available information; use restrictions could be imposed to prevent police from this kind of intrusive investigation.[11] Law enforcement officers often need to search cell phones or computer hard drives that contain enormous amounts of information, making the particularity requirement for warrants obsolete; use restrictions can ensure that the law enforcement officers only see (or can only use) the information that is truly responsive to the warrant.[12] And political concerns about terrorism have pressured law enforcement officers to seek to adopt ever more aggressive investigative tools to prevent acts of mass destruction; use restrictions could ensure that the government

7. *But see* Indianapolis v. Edmond, 531 U.S. 32, 48 (2000) (holding that in evaluating special needs searches, courts should look to the "programmatic purpose" of the government search regime).

8. Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, FUTURE OF THE CONST., Apr. 2011, at 3 https://www.brookings.edu/research/use-restrictions-and-the-future-of-surveillance-law/ [https://perma.cc/4SNH-XVSE]. Professor Kerr argues that use restrictions should come from statutes, not from the Fourth Amendment.

9. Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH. L. REV. 1, 4–5 (2015); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 64 (2014).

10. *See infra* notes 189–215 and accompanying text.

11. *See infra* notes 51–78 and accompanying text.

12. *See, e.g.*, United States v. Ganias, 755 F.3d 125, 137–39 (2d Cir. 2014) (restricting the government's authority to search the mirror image of a hard drive that had already been seized); United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 996 (9th Cir. 2009) (en banc), *revised by* 621 F.3d 1162, 1174 (9th Cir. 2010) (placing a use restriction on law enforcement officers searching a hard drive).

has access to these tools if they are necessary to combat terrorism, but prohibit them from using the tools for general crime control.[13]

But for all the recent scholarly attention that use restrictions have received, they are still not fully understood. The term "use restriction" has been used to describe a number of different types of regulations on how law enforcement can utilize information, some of which are doctrinally sound, but many of which are not consistent with current Fourth Amendment jurisprudence. Use restrictions can be legally derived from a variety of sources, depending on the context. Most fundamentally, use restrictions often create more problems than they solve. Although at first pass use restrictions seem to be elegant and sophisticated solutions to modern Fourth Amendment puzzles, closer examination reveals that they involve significant risks and may be less effective than they first appear.

Part I of this Article defines use restrictions and categorizes five different models of use restrictions. It also examines the three different sources that could (and in some cases, have already) become the legal foundations for use restrictions. Part II examines eight different contexts where use restrictions have been proposed or are tentatively being utilized, such as DNA databases or digital searches. Part III offers a critique of use restrictions by discussing the practical, doctrinal, and political problems inherent in adopting use restrictions, and argues that in many cases use restrictions would result in bad policy. In a brief conclusion, the Article argues that use restrictions promise much more than they can deliver, and that in most cases they will do more harm than good.

I. WHAT IS A "USE RESTRICTION?"

For the purposes of this Article, we will define "use restrictions" as any legal restriction—whether constitutional, statutory, or regulatory—constraining what law enforcement officials do with information already in their possession.[14] Law enforcement officials may have obtained such information through surveillance that does not implicate the Fourth Amendment (such as watching individuals in

13. *See, e.g.*, Kerr, *supra* note 8, at 3, 7–8.

14. This is similar to other definitions used by scholars. *See, e.g., id.* at 3 (defining "use restrictions" as "rules that strictly regulate what the government can do with information it has collected and processed"); Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 51 (1995) (arguing that use restrictions should "confine[] the governmental authorities to uses consistent with the [Fourth] Amendment's reasonableness requirement").

a public place);[15] through actions taken pursuant to a warrant exception or the execution of a warrant; through information obtained from a third party; or through information obtained from other government officials. Use restrictions can be contrasted with collection restrictions, which regulate how law enforcement officers gather the information—and which, as of now, remains the primary way in which the Constitution and legislatures regulate government surveillance.

The idea of use restrictions is not new. In 1995, Professor Herald Krent proposed adopting a use restriction regime, arguing that the "reasonableness" of a law enforcement seizure should be judged based on how the government subsequently uses the information obtained from the seizure.[16] Specifically, Krent argued that the courts should ban any subsequent use of the information that was not disclosed to the owner or at least implicit at the time of the seizure.[17] He used two examples in his article: DNA evidence and items recovered from lockers during school searches.[18] But Krent saw many potential future applications of his proposal, and pointed out that "[g]overnmental officials may, as technology changes, acquire increasing amounts of information about individuals."[19]

Professor Krent's proposal lay dormant for the better part of two decades, as courts ignored the idea and other scholars paid it only passing interest.[20] Commentators most often cited the benefits of use restrictions in the context of DNA databases, arguing that government agencies that collect DNA evidence for the purpose of verifying an individual's identity should be barred from using the

15. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281–82 (1983) (allowing the government to monitor the movement of a car during one trip over public roads).

16. *See* Krent, *supra* note 14, at 52.

17. *Id.* at 53, 85–92.

18. *Id.* at 93–99.

19. *Id.* at 53.

20. One exception was Professor Stephen Henderson, who argued in a 2005 article that special needs searches could become more reasonable if government agents who engage in surveillance for a certain purpose, such as looking for drugs in schools or preventing terrorism, did not share the information with law enforcement officials. Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Searches*, 56 MERCER L. REV. 507, 559–62 (2005). I also advocated use restrictions in the narrow context of anti-terrorism searches, arguing that one way of justifying suspicionless searches at airports and courthouses would be to prohibit the government from using any evidence that resulted from those searches in a future criminal trial, thus ensuring that the purpose of the search was limited to deterring terrorism. Ric Simmons, *Searching for Terrorists: Why Public Safety Is Not a Special Need*, 59 DUKE L.J. 843, 915–19 (2010).

evidence for any other purpose.[21] In recent years, however, the idea of use restrictions has been gaining traction. In 2011, Professor Orin Kerr wrote that the "future of surveillance is a future of use restrictions—rules that strictly regulate what the government can do with information it has collected and processed."[22] Over the next few years many other scholars agreed, arguing that "the age of big data calls out for a new approach."[23] Use restrictions are now seen as a way to regulate not only DNA samples[24] but also the application of big data in criminal investigations,[25] the breadth of digital searches,[26] drone surveillance,[27] and national security surveillance.[28]

A. Different Types of Use Restrictions

As seen in Part II, those who argue in favor of use restrictions make compelling practical arguments as to how this new paradigm could resolve some of the trickiest Fourth Amendment issues currently faced by the courts. But before proponents can discuss the practical applications of use restrictions, they must first provide a doctrinal basis for adopting this new approach to regulating surveillance. In other words, we need to determine what legal theory supports restricting the government's use of data that it has legally obtained. So far, the various proponents have put forward five different theories supporting the imposition of use restrictions:

(i) Applying an **"ongoing seizure"** doctrine;

(ii) Creating a purpose test for the **exclusionary rule**;

(iii) Defining the **data processing** itself as a "search";

---

21. *See, e.g.*, Wayne A. Logan, *Policing Identity*, 92 B.U. L. REV. 1561, 1605–06 (2012).

22. Kerr, *supra* note 9, at 3. (arguing that use restrictions should come from statutes, not from the Fourth Amendment).

23. Joh, *supra* note 9, at 63–65.

24. *See generally* Tracey Maclin, *Government Analysis of Shed DNA Is a Search Under the Fourth Amendment*, 48 TEX. TECH L. REV. 287 (2015) (exploring Fourth Amendment implications of government analysis of covertly collecgted DNA).

25. Joh, *supra* note 9, at 63–65; Stephen E. Henderson, *Our Records Panopticon and the American Bar Association Standards for Criminal Justice*, 66 OKLA. L. REV. 699, 722–23 (2014).

26. Kerr, *supra* note 9, at 48 (arguing for a use restriction for non-responsive files in computer warrant searches).

27. Caren Myers Morrison, *Dr. Panopticon, or, How I Learned to Stop Worrying and Love the Drone*, 27 J. CIV. RTS. & ECON. DEV. 747, 758 (2015).

28. *See* Russell D. Covey, *Pervasive Surveillance and the Future of the Fourth Amendment*, 80 MISS. L.J. 1289, 1303–05 (2011) (arguing that given the destructive power available to criminals today, the government needs to aggressively use surveillance technology, and the only way to allow this and maintain basic civil liberties is to limit the use of the information that is gathered).

(iv) Making the expected **future use** of the data collection a factor in determining whether the collection itself is constitutional; or

(v) **Sequestering** the information to specific government agencies.

Each of these theories has different benefits and drawbacks, and none of them are mutually exclusive. Thus, courts (and legislatures) could adopt any or all of them, depending on the context.

1. "Ongoing Seizures"

The first doctrinal basis to support the imposition of use restrictions would be for courts to hold that the improper use of legally gathered information transforms the legal seizure into an illegal one. This was Professor Krent's initial proposal regarding the use of DNA that had been legally collected[29] and it has found some support in more modern scholarship. For example, a recent article by Professor Kerr proposed use restrictions on warrant-authorized searches of digital evidence.[30] Kerr argues that when the government (lawfully) seizes a computer and its data pursuant to a warrant, the government's continued retention of that data is an ongoing seizure.[31] Courts agree that the initial seizure of that data will necessarily include data that is authorized by the warrant and data that is not authorized by the warrant, since all the information will be commingled in the suspect's computer.[32] Thus, the initial seizure of unauthorized data is inevitable and constitutional.[33] However, once the government starts sifting through the data, it will begin to separate the data authorized by the warrant from the unauthorized data. If the government later uses the unauthorized data, it exceeds the scope of the warrant and its ongoing seizure of the unauthorized data becomes unconstitutional.[34] As we will see in Part II, the "ongoing seizure" argument can apply to use restrictions in many other contexts in which the government legally collects and then retains data (such as DNA databases) or information shared with third parties (such as phone records or search engine queries).

29. Krent, *supra* note 14, at 53.
30. Kerr, *supra* note 9, at 17–18.
31. *Id.* at 24–29.
32. *Id.* at 11–12.
33. *Id.*
34. *Id.*

2. Linking the Exclusionary Rule to the Purpose of the Search

The second way to impose use restrictions would be to broaden the exclusionary rule[35] so that it would bar the use of any evidence that was inconsistent with the initial purpose of the search. In other words, if the court permits the government to conduct a search in order to fulfill a certain purpose, then the government can only use the results of that search for that specific, articulated purpose. The results would be inadmissible if used for any other purpose.[36]

This justification of use limitations would not apply to most searches, since Fourth Amendment jurisprudence generally focuses only on the level of suspicion possessed by the law enforcement officer and is unconcerned with the reason why the officer conducted the search. However, there is a category of Fourth Amendment searches—special needs searches—which are entirely dependent on the purpose of the search.[37] For example, the government does not need to show any level of individualized suspicion before setting up a roadblock to stop drivers, as long as the purpose of the roadblock is to detect drunk drivers and keep the roads safe.[38] Under traditional Fourth Amendment law, any information that is recovered as a result of a stop is admissible for any purpose, even though the stop was only authorized for a limited purpose.[39] But under a use limitation theory of the exclusionary rule, the evidence recovered could not be used in any case unrelated to the purpose of the special needs search. Returning to the example, if the roadblock was constitutionally permissible only because of the special need to apprehend drunk drivers, any evidence obtained during the stop would only be

35. Under the exclusionary rule, the government is prohibited from introducing evidence that was obtained in violation of a defendant's constitutional rights, unless one of the many exceptions to the rule applies. *See generally* Mapp v. Ohio, 367 U.S. 643 (1961) (establishing the exclusionary rule for all state court criminal cases).

36. Covey, *supra* note 28, at 1311–12 ("When any type of state search or seizure activity that normally would be subjected to traditional Fourth Amendment standards is exempted from those standards under the administrative or special needs doctrines, the state's right to use information obtained thereby should be restricted to the purposes that justified the exemption in the first place.").

37. *See, e.g.*, Camara v. Mun. Court, 387 U.S. 523, 537 (1967) (holding that probable cause for a health inspector to enter a home is lower because the purpose of the search is not related to traditional law enforcement).

38. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990); *but see* Indianapolis v. Edmond, 531 U.S. 32, 48 (2000) (stating roadblocks are not permitted for purely law enforcement purposes, such as searching for narcotics).

39. *See, e.g.*, Whren v. United States, 517 U.S. 806, 812–13 (1996) (noting that even if the legal justification of the stop were a pretext, the police would still be allowed to use any evidence they obtained from the stop as long as the initial justification for the stop was legal).

admissible to prove the defendant was driving while intoxicated—so any drugs, illegal weapons, or other contraband found during the roadblock would be excluded from evidence. In some ways this doctrine would be a sensible limitation on special needs searches, but as we will see below,[40] it would have far-reaching (and politically unappetizing) implications for anti-terrorism searches.

3. Broadening "Fourth Amendment Searches" to Include Processing or Distributing Data

A third legal justification of use restrictions would be to broaden the definition of a Fourth Amendment "search"[41] to include not just the collection of data but also the actions that the government takes with the data after the collection has occurred. Many commentators have proposed this as an antidote to the vast amounts of data that are currently being legally collected by the government in different contexts, such as the DNA taken from arrestees that ends up in government databases and the metadata from phone calls that is collected by third parties and handed over to criminal investigators.[42] Under this theory, the processing of the data the government legally possesses would be considered a search in its own right. Thus, the government would need to obtain a warrant or demonstrate reasonableness to a court before processing the data. This is similar to, but distinct from, the "ongoing seizure" doctrine discussed earlier. Under the "ongoing seizure" doctrine, information can be validly seized at one point in time pursuant to a warrant and then used only for a specific purpose—any further use of the seized data would constitute a new Fourth Amendment seizure under the law and would thus require a new warrant. Under the processing or distributing data doctrine, the original seizure of the information poses no Fourth Amendment issues, but any sophisticated processing or extensive sharing of the information would be considered a Fourth Amendment search.

This broader definition of "search" is not consistent with existing Fourth Amendment doctrine,[43] and also requires courts to draw difficult lines about the point at which a further use of already-collected data becomes a new search. For example, if a computer

40. *See infra* notes 247–48 and accompanying text.

41. U.S. CONST. amend, IV ("The right of the people to be secure . . . against unreasonable searches . . . shall not be violated . . . .").

42. *See, e.g.*, Logan, *supra* note 21, at 1605–06 (arguing that the courts should restrict the use of "identity information" that the government possesses).

43. *See infra* Section III.A.1.

processes information but does not share it with human beings, has a second "search" occurred? What about when police aggregate data to predict the location of future criminal activity?

4. Evaluating a Search Based on the Expected Future Use of the Data

The fourth proposed basis for creating use restrictions is similar, but subtly distinct. It involves courts evaluating the constitutionality of a search, in part by looking to the purpose for which the information will later be used. This type of use restriction requires less of a doctrinal shift than the previous method, since the definition of a Fourth Amendment "search" will still refer to the collection of data, not its actual use. Under this doctrine, the courts will look to the *purpose* of the search as well as the *manner* of the search.

Courts already apply this type of use restriction when they analyze searches under the special needs doctrine. When the government collects certain information for a non-law enforcement purpose, such as conducting drug tests on train operators to ensure the safety of train passengers, courts will apply the more lenient "reasonableness" standard rather than the higher standard of probable cause.[44] So far, courts have only applied this sort of use restriction in the context of special needs[45]—that is, asking whether the purpose of the search is to advance a law enforcement goal or to further some other goal. A more aggressive application of use restrictions could be imposed to create many different kinds of distinctions between different proposed uses. For example, courts could hold that collecting DNA for the purposes of establishing an arrestee's identity was a reasonable search, but collecting DNA for the purposes of learning more intimate details about the suspect would be an unreasonable search.[46]

5. Sequestering

Finally, courts or legislatures could restrict access to the previously collected information based on the government agency's seeking the information. This limitation usually means sequestering

---

44. *See, e.g.*, Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 618–20 (1989) (applying the "reasonableness" standard rather than the warrant requirement or the probable cause standard); *see also infra* Part II.C.

45. *See infra* notes 97–126 and accompanying text.

46. In fact, some have argued that the Supreme Court did exactly this in *Maryland v. King*, 133 S. Ct. 1958, 1977 (2013) (allowing the gathering of DNA evidence from arrestees if the information is used for identification purposes). *See infra* Section II.B.

law enforcement agencies—creating a "wall" between the non-law enforcement agency that gathered the information (and can generally use it for whatever purpose that is within its agency's mandate) and law enforcement. For example, if the National Transportation Safety Board ("NTSB") were to require all self-driving cars to report their location to the government at all times in order to ensure safety on the roadways, the NTSB could only use the location information for the purpose of ensuring safe roads and could not share it with law enforcement officials for crime control purposes. As different branches of the government gather increasing amounts of information for diverse purposes, the imposition of this type of use restriction could be a way to allow other agencies to continue doing their job while still preventing law enforcement from gaining access to a vast and growing database of private information.

B. Different Methods of Creating Use Restrictions

Any of the five identified use restrictions would need a basis in legal authority to be imposed on law enforcement conduct. There are three potential sources of legal authority that can be used to justify use restrictions.

First, courts could interpret the Fourth Amendment as requiring certain types of use restrictions. With respect to the first three types of use restrictions, this would require a radical shift in Fourth Amendment doctrine, which currently regulates searches and seizures at the collection stage rather than at any subsequent stage. And as with any new doctrine, it would require a significant amount of litigation as the Supreme Court and then various circuit courts carved out the scope of the various forms of use restrictions one case at a time.

Second, magistrates and district court judges could impose use restrictions into search warrants as a way of complying with the particularity requirement of the Fourth Amendment.[47] This poses less of a doctrinal challenge, since magistrates and judges who issue warrants have broad discretion to add in specific requirements when crafting warrants, and there is no legal reason why use restrictions could not be part of these requirements. However, since this method imposes use restrictions into warrants, it is obviously limited to situations in which the government is already seeking a warrant, and so it would not affect the vast majority of surveillance that occurs. It is

47. *See* U.S. CONST., amend. IV (requiring all warrants to "particularly describe[]" the place to be searched and the persons or things to be seized).

probably most useful for the third type of use restriction—the "ongoing seizure"—since many of those seizures are made pursuant to a warrant. This process of creating use restrictions would probably involve circuit court judges enforcing the particularity clause to overturn warrants which did not include a use restriction, thus forcing district court judges and magistrates to routinely include use restrictions when issuing warrants.

Finally, legislatures could create use statutes which require restrictions in certain contexts. This would also pose no challenge to current Fourth Amendment doctrine, and it would allow legislatures to fine-tune use restrictions to very narrow factual contexts. And as we will see, legislatures have already created numerous use restrictions in the areas of criminal justice and privacy.[48] However, encouraging legislatures to create use restrictions would end up further complicating search and seizure doctrine, making it harder for law enforcement officials to know how they could legally use their collected data in different contexts. Additionally, different state legislatures could craft different solutions for their jurisdictions, leading to a lack of uniformity.[49] Furthermore, legislatures may face strong political resistance if they try to impose use restrictions in certain contexts.[50]

II. POSSIBLE APPLICATIONS FOR USE RESTRICTIONS

The previous Section examined how use restrictions could be created—both the potential doctrinal basis for use restrictions and the practical ways that they could be enacted into law. This Part turns to the next question: how would use restrictions be used? In other words, in what factual scenarios would use restrictions be helpful, what are the pros and cons of adopting use restrictions in each of these areas, and to what degree have courts already adopted use restrictions? Over the past few years, use restrictions have been proposed in many different contexts as a way to solve numerous seemingly intractable Fourth Amendment problems. In some areas, courts and legislatures have already moved towards adopting a

48. *See infra* Section III.A.2.

49. This lack of uniformity is also an issue when state courts interpret their state constitutions to give greater protections than the federal constitution, but the complications multiply significantly with the entry of state legislatures into the picture.

50. Use restrictions would mean that in some situations law enforcement officers who possessed evidence of criminal activity could not use that evidence to prove that the perpetrator committed the crime. This limitation would be politically unpopular with many voters. *See infra* text accompanying note 248.

version of use restrictions in evaluating the constitutionality of the government action. This Part provides an overview of eight different contexts in which use restrictions are becoming a reality: the mosaic theory doctrine, DNA databanks, special needs searches, national security, digital searches, drones and body cameras, the binary search doctrine, and encryption.

A. Mosaic Theory

The mosaic theory is a relatively new concept that has been garnering a considerable amount of attention among commentators[51] and has begun to gain traction in the Supreme Court.[52] The mosaic theory holds that aggregating many small, seemingly innocuous bits of data about a person can reveal detailed, intimate information about a person's life.[53] The small bits of data could take on many forms, such as the individual locations that a person visits, metadata about telephone calls or internet uses, or specific credit card purchases.

The implications of the mosaic theory for Fourth Amendment doctrine are profound, since the government can often collect these small bits of data without implicating the Fourth Amendment. Often, individuals share these data points with third parties, and thus the data are freely available to the government under the third-party rule.[54] In other contexts, the data consists of information in which the individual never had any reasonable expectation of privacy in the first place, such as a person's location in a public place[55] or address

51. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 314 (2012); *see also* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 390 (2013); Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y (SPECIAL ISSUE) 1, 4 (2012).

52. Riley v. California, 134 S. Ct. 2473, 2489 (2014) (noting that one of the reasons cell phones require more protections than other "containers" is that the distinct types of information in the phone can "reveal much more in combination than any isolated record"); United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *see also infra* note 66 and accompanying text. Although *Jones* and *Riley* hinted that the Court was moving towards adopting the mosaic theory, the Court has not yet formally adopted the doctrine.

53. As two commentators recently described it, the mosaic theory holds that "we can maintain reasonable expectations of privacy in certain quantities of information and data even if we lack reasonable expectations of privacy in the constituent parts of those wholes." *See* Gray & Citron, *supra* note 51, at 397.

54. The Supreme Court has held that an individual has no reasonable expectation of privacy in any information that she provides to a third party. Smith v. Maryland, 442 U.S. 735, 743 (1979) (applying the third-party doctrine to phone numbers dialed on a telephone call).

55. United States v. Knotts, 460 U.S. 276, 281–82 (1983).

information on an email.[56] Thus, the collection of each individual piece of information does not implicate the Fourth Amendment, but under the mosaic theory, aggregating them together in certain ways becomes a "search" and thus would implicate the Fourth Amendment.

The mosaic theory has become more significant as technology has allowed for more bulk collection of data by the government and private companies. The growing literature about the use of "big data" by law enforcement is yet another manifestation of applying the mosaic theory to the Fourth Amendment.[57] The use of big data raises a number of interesting questions, such as whether, and to what degree, predictive algorithms can be used to create reasonable suspicion or probable cause.[58] But even before courts reach those questions, they will have to decide whether the bulk collection and/or processing of the information constitutes a Fourth Amendment search.

Courts could incorporate the mosaic theory into Fourth Amendment doctrine in two different ways. First, courts could rule that the Fourth Amendment restricts the bulk *collection* of data; that is, even though collecting any single piece of data may not be a search, collecting hundreds of pieces of the same type of data would be a search. This is essentially the Fourth Amendment theory that was adopted by the four concurring Justices in *United States v. Jones*[59] who held that continuously tracking a suspect's movements along public roads for twenty-eight days is a search.[60]

---

56. United States v. Forrester, 495 F.3d 1041, 1048–50 (9th Cir. 2007).

57. *See generally* Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461 (2015) (arguing that the use of big data conflicts with the individualized suspicion requirement of the Fourth Amendment); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015) [hereinafter Ferguson, *Reasonable Suspicion*] (imagining the use of big data by police on the street to determine whether reasonable suspicion exists for a *Terry* stop); Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259 (2012) (examining how big data can be used by police to generate reasonable suspicion); Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15 (2016) (arguing for more accountability in the way police use big data to allocate their surveillance resources); Joh, *supra* note 9 (defining "big data" as the application of artificial intelligence to vast amounts of digitized data).

58. *See* Ferguson, *Reasonable Suspicion*, *supra* note 57, at 388–403; Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 969–83 (2016).

59. 565 U.S. 400 (2012).

60. *Id.* at 429–31 (Alito, J., concurring). The majority opinion based its conclusion that there was a search in this context on a trespass-based theory: since the government physically placed a GPS tracker on the individual's car, a search had occurred. *Id.* at 404–05 (majority opinion).

This interpretation of the Fourth Amendment presents serious challenges to current Fourth Amendment doctrine. If collecting one point of data is not a search, how could collecting a series of the same type of data become a search? At what point does a series of non-searches suddenly become a search?[61] Courts could answer these questions by applying *Katz*'s "reasonable expectation of privacy" test in every context in which the mosaic theory applies.[62] For example, a court could rule that a suspect's reasonable expectation of privacy is violated when the police track public movements for twenty-eight days, or collect over twenty search engine queries over a one-week period, or collect six months' worth of phone records. But this approach would require dozens of different cases to set out the parameters of the theory and could result in disparate standards that would create ambiguity or inconsistency.[63]

The second option of incorporating the mosaic theory is to turn to use restrictions. Under this option, the rules on collecting data would remain the same: obtaining data from public sources or third parties would not be a search regardless of the volume of data which is collected. But aggregating the data and drawing conclusions from those aggregations would be deemed a search. This is an example of the "data processing" rationale.[64] The aggregation could be relatively unsophisticated, such as a police officer reviewing an entire month's worth of GPS data to determine patterns and deviations from those patterns. Or it could be more complex, such as the software used by the National Security Administration that sifts through millions of cell phone records to predict criminal activity. In any case, the courts would consider the aggregation to be a separate search and then

61. *See* Kerr, *supra* note 51, at 333–34. Professor Kerr focuses on four problems that the mosaic theory creates for Fourth Amendment jurisprudence. First, what is the standard for determining when a "mosaic" is created? Second, what types of grouping count as making a mosaic? Third, how is it determined when a mosaic is "reasonable," especially given the fact that all of its constituent parts are reasonable on their own. And fourth, what is the remedy for mosaic searches? *Id.* at 329–30.

62. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

63. Professor Christopher Slobogin has proposed a statute that would codify when an otherwise innocuous surveillance becomes a Fourth Amendment search under the mosaic theory. Slobogin, *supra* note 51, at 24. His proposal relies on restricting the surveillance at the collection stage, for example: "[a] targeted public search that lasts longer than 20 minutes in aggregate but no longer than 48 hours in aggregate requires reasonable suspicion." *Id.* at 24.

64. *See supra* Section I.A.3.

analyze whether that aggregation represented a Fourth Amendment violation.

Just like the more traditional model of the mosaic theory advocated by the *Jones* concurrence, the data-processing use restriction of adopting the mosaic theory would require a revision of Fourth Amendment doctrine, since the Fourth Amendment has traditionally only applied to the data collection phase of the investigation. However, this rationale could avoid the problem of drawing arbitrary lines about the exact point at which massive data collection becomes a search. In this way, adopting a use restriction theory of the Fourth Amendment could legitimize and simplify the mosaic theory. Courts would no longer need to restrict the length of the surveillance or determine how many different data points would constitute a search. Instead, courts would focus on how law enforcement officers grouped the different data points together. If law enforcement officers wanted to obtain massive amounts of public information, the Fourth Amendment would allow such acquisition. And if a law enforcement officer then needed to look at one piece of that information—that is, to determine whether the suspect was at a certain place at a certain time, or whether he placed a phone call to a certain person on a specific day—the officer could verify that without violating the suspect's rights. But if the law enforcement officer utilized the entire packet of information to seek out patterns, or used a software algorithm to determine probable cause, she would be conducting a Fourth Amendment search.

Of course, this application of the Fourth Amendment still requires courts to determine which types of data aggregation constitute a search, but these distinctions would be easier and more intuitive to draw because they would be more closely tied to the *results* the law enforcement officers obtain rather than the *actions* that the officers take. Take the example of *Jones*. The concurrence in *Jones* told us that twenty-eight days of surveillance along public roads is a search.[65] This leaves lower courts and police officers with the inevitable question of whether twenty-five days of surveillance is permissible, or fifteen days, or ten days. Not only are such distinctions arbitrary, they miss the point of the mosaic theory. The real privacy invasion that the mosaic theory seeks to address is not the amount of information that the government obtains; it is the information that law enforcement is able to learn from looking at the patterns from the

65. United States v. Jones, 565 U.S. 400, 413 (2012) (Sotomayor, J., concurring); *id.* at 430–31 (Alito, J., concurring).

aggregated data. It would make more sense for a court to examine how the law enforcement officers analyze the information—what conclusions they are capable of drawing given their analysis—and determine whether the information from that analysis violates the suspect's reasonable expectation of privacy. This, after all, is the rationale behind the mosaic theory: that through aggregating data, new truths (or at least probabilities) can be gleaned from otherwise harmless information.[66] Applying a use restriction to the information would place a court's focus where it belongs: on the aggregation of the data, not its original collection.[67]

Although applying use restrictions seems to present courts with an elegant way out of the doctrinal dilemma posed by the mosaic theory, courts have been reluctant to move in this direction. *Jones* is the only Supreme Court case that has touched on collecting large amounts of data, and the Justices for the most part refused to adopt a use restriction analysis when applying the mosaic theory. The four concurring Justices that adopted a version of the mosaic theory explained that it was the "prolonged" nature of the surveillance that made it a Fourth Amendment search, arguing that society's reasonable expectation has traditionally been that law enforcement agents could follow a person on one trip, but they would not and could not monitor a person's movements for an extended period of time.[68] In other words, they focused on the bulk *collection* of the data and did not concern themselves with what the government did with the data once it had been collected. Only Justice Sotomayor hinted that what the government *did* with the data raised Fourth Amendment concerns; and this was a very subtle hint indeed.[69]

Lower courts have also been disinclined to apply a use limitation in cases invoking extensive data collection. Before the *Jones* case was

66. *See* Kerr, *supra* note 51, at 313.

67. For many privacy advocates, however, utilizing use restrictions to justify the mosaic theory is insufficient, since law enforcement officers would be permitted to possess enormous stores of data about anyone they chose to monitor. The mere fact that the government holds this information—even in raw form, and even if no member of law enforcement actually ever looks at it—could still be seen as an infringement of privacy. Furthermore, there is a question of enforcement: just because the police are not permitted to examine this information in the aggregate without a warrant does not mean that all members of law enforcement will follow this rule. These critiques (which are common to nearly every type of use restriction) are considered in Part III.

68. *See* 565 U.S. at 430 (Alito, J., concurring).

69. *See id.* at 416 (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded *and aggregated* in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." (emphasis added)).

appealed to the Supreme Court, the D.C. Circuit held that the twenty-eight-day surveillance of the defendant was a Fourth Amendment search, and even cited the mosaic theory as one of the reasons why the prolonged warrantless surveillance violated the defendant's rights.[70] But the court stopped short of embracing a use restriction theory, instead focusing on the concept that the government could see a broader view of the defendant's life, revealing patterns of conduct instead of isolated trips. The closest the D.C. Circuit came to mentioning any kind of use restriction was its statement that an individual expects each of his movements to remain "disconnected and anonymous," and by connecting the separate trips together, law enforcement transforms individual legal searches into an intimate portrait.[71] Thus, one could argue that monitoring many separate trips is not a search, but the act of "connecting" the trips together after the monitoring becomes a search. But this seems like a stretch; what the D.C. Circuit was really objecting to (like the Supreme Court concurrences later) was the prolonged nature of the surveillance, not the manipulation or processing of the data afterwards.

Even courts presiding over cases that review extremely massive amounts of surveillance data have refused to adopt use restrictions on the government. In recent years there have been a spate of lawsuits surrounding the Internet surveillance conducted by the National Security Agency ("NSA").[72] In one of those cases, a district court judge granted an injunction against the NSA, arguing that the third-party doctrine no longer applies in the context of bulk collection of metadata.[73] Although the court did briefly discuss the data mining that the government was able to perform,[74] it based its ruling on many

70. United States v. Maynard, 615 F.3d 544, 561–63 (D.C. Cir. 2010), *aff'd sub nom.*, United States v. Jones, 565 U.S. 400 (2012).

71. *Id.* at 563 (Breitel, J., concurring) (quoting Nader v. Gen. Motors Corp., 255 N.E.2d 765, 772 (N.Y. 1970)).

72. The group ProPublica has compiled a list of approximately forty lawsuits that have been filed since 2006 regarding the NSA's mass surveillance program. *See* Kara Brandeisky, *NSA Surveillance Lawsuit Tracker*, PROPUBLICA (July 10, 2013), https://projects.propublica.org/graphics/surveillance-suits (last updated May 13, 2015) [http://perma.cc/3SNB-NZC3]. These lawsuits can be roughly divided into three categories: lawsuits that seek to compel the NSA to release information about its surveillance programs; lawsuits by criminal defendants who are challenging the use of covert NSA surveillance in their criminal case; and lawsuits that claim that the NSA surveillance violates the NSA's statutory authority and/or the Constitution.

73. Klayman v. Obama, 957 F. Supp. 2d 1, 30–38 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

74. *Id.* at 33 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)) ("[T]he Government has at its disposal today the most advanced twenty-first century tools,

other factors as well, including the length of time that the NSA program was collecting information, the close cooperation between the government and the third-party companies who provided the information, and the "nature and quantity" of the information that was being gathered.[75] Meanwhile, a district court judge in New York ruled that the NSA surveillance program did not violate the Constitution, regardless of what the government did with the massive amounts of information that it collected.[76]

In short, even though use restrictions would be an elegant and sensible way to justify applying the mosaic doctrine, so far courts have been reluctant to adopt this new approach to applying the Fourth Amendment. This same judicial reluctance exists in other areas where adopting use restrictions would seem sensible, including regulation of DNA evidence[77] and the application of the special needs doctrine.[78]

B. DNA Databanks

Professor Krent's original article cited DNA samples as one of the primary contexts in which use restrictions would be useful.[79] This is an especially compelling area for use restrictions for a number of reasons: DNA samples are easily collected, they serve a critical non-intrusive purpose (establishing identity), and they contain vast amounts of information that could reveal intimate details about a person. But the best argument for use restrictions in this context is the paucity of constitutional restrictions on the collection of DNA samples. Taking a DNA sample directly from a person's body is considered a "search," but the Court has found such a search to be reasonable when conducted on an individual who has been arrested for a felony.[80] More significantly, the collection of "abandoned" DNA—genetic material that is unavoidably left behind in public places—is completely unregulated by the Fourth Amendment.[81] Thus, DNA represents a type of information which is: (1) easily accessible

---

allowing it to 'store such records and efficiently mine them for information years into the future.'").

75. *Id.* at 30–38.

76. ACLU v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013), *aff'd in part, vacated in part, and remanded*, 785 F.3d 787 (2d Cir. 2015).

77. *See infra* Section II.B.

78. *See infra* Section II.C.

79. *See* Krent, *supra* note 14, at 93–97.

80. *See* Maryland v. King, 133 S. Ct. 1958, 1980 (2013).

81. *See, e.g.*, State v. Athan, 158 P.3d 27, 37 (Wash. 2007) (en banc) (finding "no cases or support" for the defendant's argument that he had a reasonable expectation of privacy in the DNA in his saliva that he voluntarily placed on an envelope).

(both practically and legally); (2) essential and uncontroversial when used for one purpose; and (3) invasive when used for other purposes. Intuitively, using DNA to establish a suspect's identity might seem "reasonable" under the Fourth Amendment, but storing it in a permanent database, using it to investigate cold cases, or analyzing it to learn more personal information about the suspect may seem less reasonable.

When Professor Krent originally proposed use restrictions for DNA evidence twenty years ago, he proposed two different ways that use restrictions could be applied to DNA evidence. First, the legality of the DNA collection could be conditioned on the presumption that the DNA would only be used in certain ways[82]—what this Article has termed the "future use" rationale.[83] If law enforcement seeks a warrant to conduct the search, this method works well because a court can set out conditions in the warrant that restrict how the information is used.[84] However, DNA samples may be obtained without a warrant,[85] thus making it difficult to impose any use restrictions at the collection stage without a significant adjustment to Fourth Amendment jurisprudence. Instead, courts would have to adopt Professor Krent's second option, which is to categorize certain uses of DNA as a separate search, distinct from the collection itself.[86] Indeed, most modern proposals for DNA use restrictions adopt this argument. Professor Wayne Logan argues that "[w]hen government uses identity evidence forensically—to investigate an arrestee's possible role in other criminal activity—a distinct government purpose (and hence search) is pursued."[87] Similarly, Professor Tracey Maclin has argued that "[g]overnment analysis of shed DNA is a search under the Fourth Amendment."[88] This rationale for use restrictions is a cross between the "ongoing seizure" model[89] and the "processing data" model.[90] If keeping millions of samples of DNA in

82. *See* Krent, *supra* note 14, at 86–93.

83. *See supra* Section I.A.4.

84. This is the argument made to justify use restrictions of certain types of digital evidence. *See infra* notes 165–183 and accompanying text.

85. See, *e.g.*, *King*, 133 S. Ct. at 1980 (allowing for warrantless collection of DNA samples from felony arrestees); *Athan*, 158 P.3d at 37 (confirming that no warrant is required to collect "abandoned" DNA).

86. *See* Krent, *supra* note 14, at 95–98 ("The fact that the government legitimately obtained the sample . . . should not be determinative. Rather, the government's planned use of the blood sample must pass the Fourth Amendment hurdle . . . .").

87. Logan, *supra* note 21, at 1605.

88. Maclin, *supra* note 24, at 312.

89. *See supra* Section I.A.1.

90. *See supra* Section I.A.3.

storage until they can be used in future cases is deemed a Fourth Amendment violation, the use restriction belongs in the "ongoing seizure" category. But if detailed analysis of the DNA is deemed a Fourth Amendment violation, the use restriction would be justified under the "processing data" rationale.[91]

As in the mosaic theory context, the Supreme Court recently had the opportunity to impose use restrictions on DNA evidence, and (at least for now) it refused to do so. In *Maryland v. King*, [92] the Court held that swabbing the inside of a suspect's mouth and then analyzing the DNA was a "search," but that the search was "reasonable" if conducted on felony arrestees.[93] The Court did note in dicta that the limited purpose of the search (identification of the suspect) was a significant factor in its determination that the search was reasonable, and the Court further noted that "[i]f in the future police analyze samples to determine, for instance, an arrestee's predisposition for a particular disease or other hereditary factors not relevant to identity, that case would present additional privacy concerns not present here."[94] Thus, the Court explicitly left open the possibility of use restrictions in a future case, and implied that the very act of analyzing samples was an independent search because such an act would "present additional privacy concerns."[95] The Court also pointed out that the Maryland law authorizing this procedure stated that "only DNA records that directly relate to the identification of individuals shall be collected and stored."[96]

However, the Court stopped short of holding that the act of analyzing the DNA constituted a search, instead rooting its argument firmly within the traditional Fourth Amendment doctrine that focuses on the act of collection.[97] In other words, the Court held that DNA

91. A similar doctrinal question arises in the context of "familial DNA searches," in which the government runs a DNA sample against a database of known criminals and finds a partial match, indicating that the person who contributed the sample is not a match, but a close family member probably is. Even if the courts decide that processing DNA is a "search" under the Fourth Amendment, it is not clear that the family member would have standing to challenge the processing, since it is the contributor's sample that is being processed. *See* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1094–95 (2016) (arguing for application of administrative law principles to regulate massive aggregation of collected data).

92. 133 S. Ct. 1958 (2013).

93. *Id.* at 1980.

94. *Id.* at 1979.

95. *Id.*

96. *Id.* at 1979–80 (quoting MD. CODE ANN., PUB. SAFETY § 2-505(b)(1) (West, Westlaw through 2017 Reg. Sess.)).

97. *Id.*

collection made for the purposes of identification was a reasonable search and implied that collection made for a different purpose might not be—the Court never stated that the *analysis* of the DNA itself was a search.[98] This is a subtle distinction, but an important one, because it demonstrates that *King* does not actually establish a doctrinal foundation for use restrictions.

In contrast to *King*, an earlier Fourth Circuit case, *United States v. Davis*,[99] held that analysis of DNA samples constitutes a search, because "the individual retains a legitimate expectation of privacy in the information obtained from the testing."[100] The *King* Court refused to explicitly adopt this position. Indeed, the Maryland Supreme Court cited *King* a year later in a case that held that analyzing DNA for the purposes of identification is not a search.[101]

C. *Special Needs Searches*

A "special needs" search is (in theory) a type of government surveillance which is undertaken for a non-law enforcement purpose. Such purposes have included ensuring the safety of railway passengers,[102] maintaining a positive learning environment in schools,[103] or securing the country's borders.[104] In practice, the line between a search pursuant to a "law enforcement purpose" and a search pursuant to a "non-law enforcement purpose" can become blurred.[105] For example, the Court approved drunk driving checkpoints for the "non-law enforcement purpose" of keeping the roadway safe;[106] while circuit courts approve searches at airports for the "non-law enforcement purpose" of maintaining airline safety[107]—even though drunk driving checkpoints and airport searches primarily

98. *But see* Maclin, *supra* note 24, at 294 (arguing that a passage in *Maryland v. King* could be interpreted to mean that subsequent analysis of a legally obtained DNA sample is indeed a search, but that under the conditions present in the case, it did not constitute an *unreasonable* search).

99. 690 F.3d 226 (4th Cir. 2012).

100. *Id.* at 243–44.

101. Raynor v. State, 99 A.3d 753, 767 (Md. 2014). Like the United States Supreme Court, the Maryland Supreme Court left open the possibility that obtaining the DNA for a purpose other than identification could be an unreasonable search. *Id.* at 768.

102. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 633–34 (1989).

103. New Jersey v. T.L.O., 469 U.S. 325, 347–48 (1985).

104. United States v. Martinez-Fuerte, 428 U.S. 543, 566–67 (1976).

105. *See* Simmons, *supra* note 20, at 887–88.

106. Mich. Dep't of State Police v. Sitz, 464 U.S. 444, 449–52 (1990).

107. *See, e.g.*, United States v. Davis, 482 F.2d 893, 911 (9th Cir. 1979), *overruled on other grounds by* United States v. Aakai, 497 F.3d 955 (9th Cir. 2007) (en banc).

exist to detect and deter criminal activity.[108] But, however blurry the line might be, the courts continue to rely on the purpose of the search as a critical factor in determining whether the search is legal.[109]

This set of rules for the special needs doctrine is a version of the "future use" rationale for use restrictions. It is not a true "future use" rationale, since the police and prosecutors are still allowed to use the results of the searches in criminal prosecutions, but it comes as close as we have seen to an actual use restriction.

As with the Supreme Court's treatment of DNA evidence in *King*, the collection of the information is still the only "search" that occurs, but the focus in evaluating the constitutionality of that search has shifted from the mechanics of the search itself to what the government plans to do with the information after it has been collected. For example, in *Ferguson v. City of Charleston*,[110] the Court invalidated a program in which a public hospital tested pregnant women for drug use and then shared the positive results with law enforcement.[111] The Court held that the fact that the results were turned over to the police "provided a basis for distinguishing our prior cases applying the 'special needs' balancing approach to the determination of drug use."[112] This doctrine was later applied to drug testing in schools as well. In *Vernonia School District 47J v. Acton*,[113] the Supreme Court approved a school's random drug testing of students participating in athletics, in part because of the limited ways in which the results were used, noting that "the results of the tests [were] disclosed only to a limited class of school personnel who ha[d] a need to know; and they [were] not turned over to law enforcement authorities or used for any internal disciplinary function."[114] Likewise, in *Board of Education. v. Earls*,[115] the Court approved of suspicionless drug testing of students who were involved in competitive extracurricular activities, pointing out that "the test results are not turned over to any law enforcement authority," and holding that "[g]iven the minimally intrusive nature of the sample collection and

108. *See* Simmons, *supra* note 20, at 872–73.
109. *Id.* at 872–86.
110. 532 U.S. 67 (2001).
111. *Id.* at 85–86.
112. *Id.* at 84; *see also* Chandler v. Miller, 520 U.S. 305, 322 (1997) (striking down drug testing for candidates for designated state offices). However, none of these cases actually contains language that states that the ultimate use of the drug test results had any bearing on the Court's holding.
113. 515 U.S. 646 (1995).
114. *Id.* at 658–60.
115. 536 U.S. 822 (2002).

the limited uses to which the test results are put, we conclude that the invasion of the students' privacy is not significant."[116]

In addition, at least one special needs case has potentially adopted the "processing data" rationale to support use restrictions. In *Skinner v. Railway Labor Executives' Association*,[117] the Court held that mandatory drug tests for railway workers constituted a search.[118] The Court noted that "analysis of urine, like that of blood, can reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic.... [I]t is clear that the collection *and testing* of urine intrudes upon expectations of privacy that society has long recognized as reasonable."[119] Commentators have cited *Skinner* as evidence that the Court recognizes that it is not just the collection of data but also its subsequent use that could constitute a search.[120]

Of course, this language from *Skinner* could be interpreted another way: that the collection and testing *together* constitutes a search—that is, it is the collection with the intent to test that makes this action an unconstitutional search, not that the collection and the testing are each independent searches. And in fact, future Supreme Court cases lend support to this alternate interpretation. *Skinner* and its companion case, *National Treasury Employees Union v. Von Raab*,[121] stand alone as the only Supreme Court cases to imply in any way that the process of testing for drugs can itself can be a search. And in the *Ferguson* case, Justice Scalia noted in his dissent that under well-established law, neither the testing of the urine nor the reporting of the results to the police could be considered a search.[122]

Unfortunately, the link to any kind of use restriction in special needs cases gets even weaker outside of the drug testing context. In

116. *Id.* at 833–34.

117. 489 U.S. 602 (1989).

118. *Id.* at 633–34; *see also* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 678–79 (1989) (holding, on the same day *Skinner* was decided, that drug testing of United States Customs Service employees was a search).

119. *Skinner*, 489 U.S. at 617 (emphasis added).

120. *See, e.g.*, Maclin, *supra* note 24, at 295–99.

121. 489 U.S. 656 (1989).

122. Ferguson v. City of Charleston, 532 U.S. 67, 92–93 (2001) (Scalia, J., dissenting) ("What petitioners, the Court, and to a lesser extent the concurrence really object to is not the urine testing, but the hospital's reporting of positive drug-test results to police. But the latter is obviously not a search. At most it may be a 'derivative use of the product of a past unlawful search,' which, of course, 'work[s] no new Fourth Amendment wrong' and 'presents a question, not of rights, but of remedies.' United States v. Calandra, 414 U.S. 338, 354 (1974). There is only one act that could conceivably be regarded as a search of petitioners in the present case: the *taking* of the urine sample.... [I]t is not even arguable that the testing of urine that has been lawfully obtained is a Fourth Amendment search.").

the significant (and growing) body of case law that makes up the special needs jurisprudence, there are no other areas in which courts attach any restrictions as to how the information is subsequently used by the government, even though such a requirement would make perfect sense in the special needs context. When the Court approved drunk driving checkpoints in *Michigan Department of State Police v. Sitz*,[123] it did so knowing full well that the results of the breathalyzers were being used in criminal prosecutions.[124] Similarly, if TSA officials recover a weapon or other contraband during an airport screening, prosecutors are free to use that evidence in court.[125] And if the police officers pull over a car near the border with the purpose of detecting illegal immigration, they are perfectly entitled to use any fruits of that stop in a criminal case.[126] Thus, the link between the special needs cases and use restrictions is weaker than it first appears.

But if the Supreme Court were to adopt a robust exclusionary rule for use restrictions on information gathered from surveillance, the most logical place to start would be in the special needs context. After all, the doctrinal basis of a special needs search is that the search is undertaken for a non-law enforcement purpose. By applying a robust "future use" doctrine and prohibiting the use of any fruits of the search in a criminal case, the Court could guarantee that the search was conducted for a non-law enforcement purpose.[127] There would be no need to try to determine the "primary purpose" of the search, nor to worry about whether law enforcement is using the special needs doctrine as a pretext to obtain evidence for a criminal case. However, up until now, the Court has shown little appetite for moving away from the traditional focus on the data collection as a search, even in the special needs context.

This is somewhat surprising because use restrictions could be a very useful tool for special needs cases. Not only would adopting use restrictions ensure that the government could not abuse special needs cases by using them as a pretext for a criminal investigation, it would

123. 496 U.S. 444, 447 (1990).

124. *Id.*

125. *See, e.g.*, United States v. $124,570 U.S. Currency, 873 F.2d 1240, 1243 (9th Cir. 1989) (stating in dicta that screeners in airports who find contraband while looking for explosives or weapons are perfectly entitled to pass the information on to government agents who would use it for general law enforcement purposes).

126. *See generally* Carroll v. United States, 267 U.S. 132, 149–50 (1925) (establishing the right of police officers to search a car they have legally pulled over if they have probable cause).

127. *See* Simmons, *supra* note 20, at 915–21.

also broaden the type of special needs searches that law enforcement could conduct.

For example, imagine a rule in which the government was not allowed to use any fruits of a special needs search in a criminal prosecution. The police could still conduct drunk driving stops, but when they caught a drunk driver, they could not arrest or prosecute him—they would merely seize him for a reasonable time to ensure that he could not endanger others, perhaps until he sobered up or until someone else could drive him to his destination. They could impose civil punishment against him, such as seizing his car or revoking his license, but they could not use any evidence from the stop in a criminal case. This would still fulfill the stated purpose of the drunk driving checkpoint—removing dangerous drivers from the public roadways—and it would be consistent with the justification of the special needs exception to the warrant requirement. The same rule could apply to searches and drug tests of students in school: students could be suspended or expelled, referred to counseling, and/or barred from extracurricular activities, but they would not face criminal charges based on anything the school recovered in the search. Once again, this would fulfill the stated purpose of the search— to maintain discipline on school grounds[128]—and ensure that the search truly is being conducted for a "special need" beyond law enforcement.[129]

Not only would use restrictions protect civil liberties by preventing the abuse of the special needs doctrine as a pretext for a

128. *See* New Jersey v. T.L.O., 469 U.S. 325, 339 (1985).

129. I originally proposed applying this type of exclusionary rule-based use restriction to all anti-terrorism special needs searches (such as searches at airports and subway stops) as a way to balance the need for protection against cataclysmic attacks and need to protect privacy rights. *See* Simmons, *supra* note 20, at 916–19. Professor Russell D. Covey proposes a modified version of this use restriction: under his theory, the state could use the fruits of a special needs search in criminal cases, but only to support criminal charges that are related to the purpose of the special needs search. Thus, if police officers create a special needs roadblock to check for drunk driving and uncover evidence of drunk driving, they can use that evidence in a drunk driving prosecution. But if they found drugs or illegal weapons in the car, they could not use that evidence in a future prosecution for possession of that contraband. Likewise, if the police recovered a gun and drugs pursuant to a special needs anti-terrorism search, they could use the gun in a prosecution for a terrorism crime, but drugs would be precluded because they were not the original purpose of the search. Covey, *supra* note 28, at 1308–12. Professor Covey correctly notes that this proposal would prevent pretextual searches, and that it would be more politically palatable than a blanket ban on using the obtained evidence in any future criminal prosecution. *Id.* at 1309. However, this solution is not as doctrinally pure as a full ban on any use of the evidence in any future criminal cases; the search will still not truly be a "special needs" search if its results are used in criminal cases.

law enforcement search, but use restrictions could also benefit law enforcement by broadening the scope of the special needs exception. In a sense, use restrictions could convert almost any type of surveillance into a special needs search. For example, assume that police in a major metropolitan area sought to reduce gun violence by instituting an aggressive stop-and-frisk policy in the city. Police would no longer need reasonable suspicion or even probable cause to perform a stop-and-frisk; they would simply set up random checkpoints at various spots in the city and perform a quick pat-down of every fifth person who walked by. If an illegal gun (or any other contraband) was found, it would be seized and destroyed, but it could not be used in any criminal prosecution, and no criminal charges would be filed against the suspect. This search regime is plainly not created with a criminal law purpose, since none of the results are ever used in a criminal proceeding—the only purpose behind the program is to decrease gun violence in the city. As long as the stops are reasonable in duration and the frisks are not unreasonably intrusive, these searches should fit within the special needs doctrine.[130] The same argument could apply to a vast array of surveillance techniques, particularly those meant to protect public safety. Truly intrusive searches, such as home intrusions, wiretapping, or interception of emails, would probably never be thought of as "reasonable" under the special needs doctrine, thus placing a limit on the government's ability to invade our privacy.

The need to conduct special needs searches—and thus the need to move towards a legitimate doctrinal justification for these searches—will only increase as our society becomes more automated and as an increasing number of industries require government monitoring and regulation. The special needs doctrine was originally

130. Under the special needs doctrine, a search or a seizure is constitutional as long as it is "reasonable." *See, e.g.*, MacWade v. Kelly, 460 F.3d 260, 269 (2d. Cir. 2006) ("[O]nce the government satisfies that threshold requirement [of an immediate purpose that is distinct from investigating a crime] the court determines whether the search is reasonable by balancing several competing considerations."). There is some question as to whether a routine suspicionless stop-and-frisk policy would be deemed "reasonable" as a special needs search. Under *Brown v. Texas*, 443 U.S. 47 (1979), the suspicionless seizure of an individual to ascertain the individual's identity violated the Fourth Amendment. *Id.* at 52. But recently courts have upheld suspicionless searches of individuals who boarded subways or public buses based on the "special need" to prevent terrorism. *See, e.g.*, Am-Arab Anti-Discrimination Comm. v. Mass. Bay Transp. Auth., No. 04-11652-GAO, 2004 WL 1682859 at *4 (D. Mass. July 28, 2004) (searches of passengers on subways and busses); *Macwade*, 460 F.3d at 275 (searches of subway passengers). The suspicionless search and seizure might be considered more reasonable if the government were not permitted to use the fruits of the search in a future criminal prosecution.

born out of the need to permit government regulators the freedom to conduct suspicionless and/or warrantless inspections[131]—indeed, no regulatory state could function if the government were forced to prove some level of individualized suspicion before conducting a routine examination of a regulated entity. In the early days of the special needs doctrine, the Supreme Court upheld suspicionless searches by health inspectors,[132] and inspectors of highly regulated industries, such as sellers of firearms[133] or mines.[134] The administrative state is growing faster than ever now, and the need to enforce those regulations through government inspections is growing as well. At the same time, new technologies are allowing the government to gather ever increasing amounts of data in order to more efficiently and more effectively regulate these industries.

Consider the example of self-driving cars. Under current estimates, millions of fully autonomous vehicles will be on the nation's roads in the next ten or fifteen years.[135] Government agencies will want to regulate this new industry quite carefully, and one easy way of obtaining the necessary data for that regulation would be to require every autonomous vehicle to record its speed and location and make that data available to the government at any time.[136] Similar recording and reporting requirements may be created for the flight paths of privately owned drones. Indeed, local governments may need to maintain a sophisticated, computerized air traffic control system in order to keep track of their movements. This data would be necessary for effective regulation, yet it would routinely give the government extraordinary amounts of data about our locations and our activities. Applying use restrictions to this data would ensure that this information, which was gathered for a regulatory purpose, could only be used for that regulatory purpose and could not be data mined for evidence of criminal activity or even accessed by law enforcement

131. *See* Camara v. Mun. Court, 387 U.S. 523, 540 (1967) (holding that no individualized suspicion is required for a health inspector to obtain a warrant to enter a home). Indeed, special needs searches were initially called "administrative searches," because they were thought to be a necessary aspect of the administrative state. *See id.* at 534. For a brief history of the origin of special needs searches, see Simmons, *supra* note 20, at 855–59.

132. *Camara*, 387 U.S. at 534

133. United States v. Biswell, 406 U.S. 311, 317 (1972).

134. Donovan v. Dewey, 452 U.S. 594, 606 (1981).

135. *See* Alexander Hars, *Forecasts*, DRIVERLESS CAR MARKET WATCH, http://www.driverless-future.com/?page_id=384 [https://perma.cc/8AF3-GEGA] (collecting estimates from various sources).

136. Stephen P. Wood et al., *The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles*, 52 SANTA CLARA L. REV. 1423, 1471–72 (2012).

personnel when investigating a specific crime—unless, of course, the law enforcement officer obtained a warrant authorizing that use.

D. National Security

One particularly distinctive type of special needs search is government surveillance conducted for national security purposes. In its simplest form, this includes physical searches meant to detect and deter terrorist activity, such as searches of all airplane passengers or everyone who enters a courthouse. As we saw in the previous Section, these physical searches fit somewhat uncomfortably into the special needs category because the supposed non-law enforcement need (to ensure the safety of airline passengers) is difficult to distinguish from a law enforcement need (to detect and apprehend violent criminals). And yet to forbid law enforcement from conducting these searches, which are perceived as being integral to the country's terrorist prevention programs, is a political non-starter. As noted above,[137] use restrictions on the fruits of these searches would be a potential solution to this dilemma, though such restrictions might be difficult to sell politically.[138]

The problem becomes even more complex when we examine national security searches more broadly. Since the terrorist attacks of 2001, the federal government has aggressively expanded its national security surveillance capabilities in dozens of different ways. The NSA began issuing subpoenas to telecommunications companies to collect telephony metadata on millions of Americans.[139] The NSA also launched the PRISM program, which collected all the digital communications traveling across the Internet that matched specific search terms.[140] Meanwhile, government applications to the Foreign Intelligence Surveillance Court (the "FISA Court") nearly tripled,

137. *See supra* Section II.C.

138. In practice, a use restriction for anti-terrorism searches would mean that when a Transportation Security Administration officer recovered a gun or a bomb from an individual trying to board a plane, the weapon could be seized, but criminal charges could not be brought against the would-be hijacker. Civil penalties could be levied against the individual, such as a fine or a five-year ban on travel, and the individual could be placed on a surveillance watch list to be monitored for future criminal activity—but most people would believe that not prosecuting such an individual is too high a price to pay for Fourth Amendment purity. For further discussion of this problem, see *infra* Section III.D.

139. *See* ACLU v. Clapper, 785 F.3d 787, 796–97 (2d Cir. 2015).

140. *See* Charlie Savage, Edward Hyatt, & Peter Baker, *U.S. Confirms That It Gathers Online Data Overseas*, N.Y. TIMES, June 6, 2013, http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html [https://perma.cc/F87T-HCSH (dark archive)].

from an average of around 670 in the 1990s to an average of over 1,850 in the ten years after 2001.[141]

This expanded counter-terrorism program created a robust debate in this country as to the appropriate balance between national security and government surveillance. Government officials defend these measures as critical to keeping the country safe,[142] while groups such as the American Civil Liberties Union and the Electronic Privacy Information Center attack the measures as incompatible with a democratic society.[143] This is, of course, the latest incarnation of the age-old tension between liberty and security.

One possible solution to this conflict would be to regulate national security surveillance at the use stage rather than the acquisition stage. Professor Kerr has argued that the combination of sophisticated data processing systems and the increased threat of terrorism leads to the conclusion that "[t]he best way to achieve the benefits of computer surveillance while minimizing the privacy risks is to place greater focus on the later regulatory stages, and in particular, the final stage of public disclosure."[144] This is an example of the "ongoing seizure" method of use restrictions, in which courts initially authorize an overly broad seizure, and then impose restrictions on which bits of information the government is allowed to use out of the vast amount data that it seized.[145] This Article discusses another

141. *See Foreign Intelligence Surveillance Act Court Orders, 1979–2016*, ELEC. PRIVACY INFO. CTR., https://www.epic.org/privacy/wiretap/stats/fisa_stats.html [https://perma.cc/Z398-G2TH].

142. Once the scope of the surveillance program came to light, the Director of National Intelligence, James Clapper, defended its existence, arguing that the "[i]nformation collected under this program is among the most important and valuable intelligence information we collect, and is used to protect our nation from a wide variety of threats." *See* Savage et al., *supra* note 140.

143. *See, e.g.*, ACLU v. NSA – *Challenge to Warrantless Wiretapping*, ACLU (Sept. 10, 2014), https://www.aclu.org/cases/aclu-v-nsa-challenge-warrantless-wiretapping [https://perma.cc/2AHU-Z79V] (detailing the ACLU court battle against the NSA's "warrantless wiretaps"); *EPIC Files Supreme Court Petition, Challenges Domestic Surveillance Program*, ELEC. PRIVACY INFO. CTR., https://epic.org/2013/07/epic-files-supreme-court-petit.html [https://perma.cc/3VF9-ABSD] (describing EPIC's court battle with the NSA over the same issue).

144. *See* Kerr, *supra* note 8, at 8.

145. Professor Kerr argues that there are four stages of computer-based surveillance: (1) data collection, (2) data manipulation by a machine, (3) human disclosure, and (4) public disclosure. Rather than define the processing of the information as a "search" (as many would argue is appropriate in the DNA testing context, or in other "mosaic theory" contexts), Professor Kerr would draw the line at his third stage—when the computer discloses the information to a human being. *Id.* at 4–6.

example of this method of use restriction in the upcoming Section on warrants for searches of digital storage devices.[146]

In reality, use restrictions are the primary way in which telephony metadata has been regulated. Before 2015, the NSA was given relatively free reign to collect and maintain vast domestic telephony databases, and the courts allowed the government to access these databases (after obtaining a court order) whenever necessary to investigate a person of interest.[147] In a sense, this was an area that was governed solely by use restrictions. The government collected millions of pieces of data and stored them for future use, and when it needed to look at the data, it would apply for a "pen/trap order"[148] to allow it to trace the details of a specific phone number.[149] As one United States official explained, "The basic idea is that it's O.K. to create this huge pond of data, but you have to establish a reason to stick your pole in the water and start fishing."[150] The problem that most commentators had with the ongoing seizure use restriction in this context was that the use restriction was not very robust, since the standard for obtaining a pen/trap order is very low.[151] But in theory, either courts or the legislature could create higher standards before allowing law enforcement officers to "start fishing" in the data pond.

The other type of use restriction that, at least in theory, could be used in the national security context is the "sequester" method. Given the fact that counterterrorism and intelligence gathering are traditionally carried out by different agencies, courts or the legislature could create a firewall between agencies, allowing agencies like the NSA or the CIA relatively free reign to collect telephony metadata or monitor internet traffic, but tightly regulating the conditions under which those agencies are allowed to share their information with the

146. *See infra* Section II.E.

147. This bulk collection of metadata was authorized by the USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88 (codified as amended at 50 U.S.C. §§ 1861–62 (2012)). Congress ended the NSA's authority to conduct these massive collections in the USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101(a)(3)(C)(ii), 129 Stat. 268, 269–70 (codified at 50 U.S.C. § 1861(b)(2) (2015)).

148. A "pen/trap order" allows the police to obtain the telephone number that was dialed by the suspect.

149. *See* Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 941 (2016).

150. *See* Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES (July 6, 2013), http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?_r=0 [https://perma.cc/VC9Y-AXNG (dark archive)].

151. The Pen/Trap statute requires merely that officers certify that "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2) (2012).

FBI or the Department of Justice. As we will see below,[152] the FISA statute establishes a weak form of sequestration by placing some restrictions on how the national security agencies can share information with law enforcement agencies.

E. Digital Searches

Use restrictions have also been proposed and utilized by courts in a very different context: to ensure that law enforcement officers do not gain access to too much information when they conduct searches of digital devices pursuant to a warrant.[153] Unlike the mosaic theory's warrantless bulk surveillances that gather millions of data points about thousands of people, searches of digital devices are smaller in scale, tied to a specific individual, and supported by a warrant.

There is a growing consensus that searches of digital media raise unique problems that are not sufficiently addressed by traditional Fourth Amendment doctrine. The basic problem is that neither physical boundaries nor the particularity requirement create sufficient limitations on the extent of a digital search. Digital devices can store vast amounts of information, much of it quite personal. As the Supreme Court noted in *Riley v. California*,[154] cell phones "hold for many Americans 'the privacies of life.'"[155] This is true for laptop computers, tablets, and many other personal devices that store gigabytes of data. Thus, a warrant that allows law enforcement officers to search through a computer is the equivalent of allowing law enforcement officers to search through hundreds of file cabinets (or even warehouses) of an individual's private information. But most of the traditional legal and physical limitations that apply to traditional searches do not exist for digital searches. In a traditional search, law enforcement officers may only look in places where the item they are searching for could be hidden; thus, if they are searching for a handgun, they cannot look in places that are too small to hold a handgun.[156] In a digital search, if police are looking for a document or picture or any piece of data, they are allowed to look anywhere on the digital device to find it.[157]

---

152. See *infra* text accompanying note 243.

153. *See, e.g.*, United States v. Ganias, 755 F.3d 125, 133–41 (2d Cir. 2014), *aff'd en banc*, 824 F.3d 199 (2d Cir. 2016).

154. 134 S. Ct. 2473 (2014).

155. *Id.* at 2494–95 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

156. *See* United States v. Ross, 456 U.S. 798, 820–21 (1982) ("A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found ....").

157. *See* Kerr, *supra* note 9, at 9.

In practice, this means that if the police obtain a warrant to search a suspect's computer for documents relating to a suspected tax fraud, the police could look through every bit of data on the suspect's computer. In theory, the particularity requirement could require a warrant which specifies either the type of document that can be seized or a date range during which the target documents may have been written, but in practice individuals can easily alter the metadata on any incriminating files so that a document may appear to be of a different type or created on a different date.[158] Acknowledging this reality, Rule 41 of the Federal Rules of Criminal Procedure creates a two-step process for seizing electronic media, stating that a warrant may permit the government to seize the entire storage medium and then later review the seized material to determine which of it is actually responsive to the warrant.[159] In other words, "over-seizing is an inherent part of the electronic search process" as government necessarily seizes "a larger pool of data that it has no probable cause to collect."[160]

There are a number of different ways to solve this "over-seizing" problem. The first is to abolish or limit the plain view exception for digital searches. Under the plain view doctrine, the Fourth Amendment does not prohibit a police officer from observing (or seizing) any item or information that is in plain view, as long as the officer has a right to be in a certain location.[161] In order to solve the problem this doctrine creates for digital searches, courts could create a "digital evidence" exception to the plain view doctrine and hold that if law enforcement officers find incriminating evidence in the digital device that is not listed in the warrant, the incriminating evidence is inadmissible in a criminal proceeding.[162] This would eliminate any

158. *See id.* at 8–11.

159. *See* FED. R. CRIM. P. 41(e)(2)(B).

160. United States v. Schesso, 730 F.3d 1040, 1042 (9th Cir. 2013) (citing United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam)).

161. Harris v. United States, 390 U.S. 234, 236 (1968) (per curiam).

162. *See, e.g.*, United States v. Comprehensive Drug Testing, 579 F.3d 989, 1006 (9th Cir. 2009) (en banc) (suggesting that magistrate judges should require the government to waive the plain view exception in digital searches); United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) (holding that any incriminating evidence that is found pursuant to a digital search which was not the subject of the warrant is inadmissible unless the discovery was "inadvertent"); *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 576–84 (2005) (arguing in favor of narrowing or eliminating the plain view exception for digital searches). Professor Kerr has recently abandoned this proposal in favor of a more narrowly tailored use restriction for digital searches. *See* Kerr, *supra* note 9, at 18–24.

incentive for police to obtain digital warrants on pretextual grounds and would likely lead to more narrowly tailored digital searches. However, such a change would entail a significant restructuring of Fourth Amendment doctrine as the plain view doctrine is a long-standing legal principle.[163] Furthermore, carving out an exception to the plain view doctrine would also not prevent the government from over-seizing the data, since the government would still copy and retain the entire hard drive for a potential search at a later time.[164] Thus, the government would still possess and see far more information than authorized in the warrant; it would simply be restricted as to how much of the information it could use in court against the defendant in a specific case.

Another possibility would be for a court issuing a warrant to place restrictions on how the warrant is executed, in order to ensure that the law enforcement officers never see any information not authorized in the warrant. The Ninth Circuit approved of such a procedure in the en banc decision *United States v. Comprehensive Drug Testing*.[165] In that case, the government sought a warrant to obtain the drug testing results of a few specific individuals in a company's database.[166] The issuing magistrate granted the warrant, but mandated specific search protocols, including the requirement that an independent group of forensic experts had to conduct the search and segregate the information specified in the warrant before handing it over to the investigating officers.[167] This is a modified version of the "sequester" rationale, since it works by keeping certain data out of the hands of law enforcement entirely. Although this solution is cumbersome, it nevertheless prevents law enforcement officers from accessing or obtaining any data that is not the subject of the warrant. The resulting search maximizes privacy rights. The disadvantage of such a solution is that it tends to balkanize criminal procedure rules regarding digital searches. Instead of appellate courts laying down broadly applicable rules regarding the types of searches that are reasonable under the Fourth Amendment, appellate courts

163. *Harris*, 390 U.S. at 236 ("It has long been settled that objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence.").

164. *Id.* at 14–17.

165. 579 F.3d 989 (9th Cir. 2009) (en banc).

166. *Id.* at 993–94.

167. *Id.* at 996.

would merely review whether each individual magistrate's search protocol was followed.[168]

A third solution would be to apply the ongoing seizure rationale to justify the exclusion of certain evidence.[169] In other words, when law enforcement seizes information from a digital device and holds the information, the continued possession of that information is an ongoing seizure, and the moment that law enforcement uses the information for a different investigation, that seizure becomes unreasonable.[170] Thus, the government should only be able to use the previously-seized information if the use is consistent with the original warrant.[171] As Professor Stephen Henderson noted: "[i]t is a serious invasion if the government can over-seize massive amounts of private information and forever retain it for indefinite later search."[172]

Use restrictions are easier to defend in the context of digital searches because the particularity requirement inherent in a search warrant essentially creates a sound doctrinal basis for restricting the data that the government is allowed to use, and thus imposing a use restriction does not require any fundamental re-working of Fourth Amendment jurisprudence.[173]

The Second Circuit imposed just such a use restriction in the case of *United States v. Ganias*,[174] in which law enforcement officers obtained a warrant to search the defendant's computers for evidence that his clients were overcharging the army for services.[175] Pursuant to standard procedure, the officers made "mirror images" of all of the defendant's hard drives, which copied every single piece of data on the computers.[176] At the time of the search, the officers told the defendant that the government was only looking for evidence of the overcharging and that everything else would be deleted once the relevant files were recovered.[177] However, once the agents obtained

168. Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1278 (2010).

169. See *supra* Section I.A.1.

170. *See* Kerr, *supra* note 9, at 18.

171. A modified version of the ongoing seizure rationale would allow the government to use the seized information if there was a national security concern or other exigent circumstances. *See* Henderson, *supra* note 149, at 948.

172. *Id.* at 947.

173. This type of use restriction would require a minor change in Fourth Amendment doctrine: recognizing the concept of an "ongoing seizure" to apply to a situation in which the government retains information that they legally obtained in a search.

174. 755 F.3d 125 (2d Cir. 2014).

175. *Id.* at 128.

176. *Id.*

177. *Id.*

the files that were listed in the warrant, they kept the full copies of the hard drives for the next two and a half years.[178] During that time the law enforcement agents developed probable cause to believe that the defendant was involved in under-reporting his client's income, and they obtained a warrant to search the stored hard drive for evidence of this new crime.[179] By that time, the defendant had altered the data on his own computer, so the only evidence of the crime was the copies of the data that the government had preserved.[180]

On appeal, the Second Circuit held that law enforcement officers violated the defendant's rights when they used the retained computer data for a purpose that went beyond that which was authorized by the original warrant.[181] The court held that the initial overly broad seizure was necessary to execute the first warrant, but that once the "responsive" files were recovered, the "non-responsive" files should have been deleted.[182] The court thus imposed a use restriction on the data recovered in the initial seizure—although all the data was legally seized, only the responsive data could be used.[183]

A similar problem, and a similar solution, arises in investigations that use cell-site simulators to collect a suspect's cell phone number. A cell-site simulator, otherwise known as a "stingray," fools all the cell phones in the immediate area into thinking it is a cell phone tower, and thereby collects identifying information from all of the nearby cell phones.[184] Law enforcement officers use these devices to learn the cell phone number of a specific suspect: they will see the suspect in a public place, activate the stingray, and obtain a list of the

178. *Id.* at 129–30.

179. *Id.* at 130.

180. *Id.*

181. *Id.* at 137–39.

182. *Id.* at 139 (conceding that the government may need to keep the entire mirrored copy of the hard drive in order to properly authenticate the responsive files, but that this was the only proper use of the non-responsive files).

183. *Id.* at 140. Many courts have held that an initial "overbroad" seizure is reasonable given the nature of electronic records. *See* United States v. Evers, 669 F.3d 645, 652 (6th Cir. 2012); Guest v. Leis, 255 F.3d 325, 334–35 (6th Cir. 2001); *In re* the Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 10 (D.D.C. 2013) (justifying the issuing of "secondary orders" when granting warrants to search electronic media, requiring that non-responsive contents must be returned or destroyed); United States v. Winther, Criminal No. 11-212, 2011 WL 5837083, at *11–12 (E.D. Pa. Nov. 18, 2011).

184. ADAM BATES, CATO INST., STINGRAY: A NEW FRONTIER IN POLICE SURVEILLANCE 4–5 (Cato Inst., Policy Analysis No. 809, 2017), https://object.cato.org/sites/cato.org/files/pubs/pdf/pa-809-revised.pdf [https://perma.cc/G9MW-SASG].

telephone numbers of all of the cell phones in the area.[185] They will then follow the suspect to another location, re-activate the stingray, and get another list of the nearby cell phones.[186] After repeating this process a few times, the agents can isolate the suspect's phone number as the only number that is consistently present at each location. The agents then obtain a pen/trap order or a wiretap order for the defendant's phone and continue their investigation.[187] But in the meantime, the law enforcement officers have collected dozens or hundreds of phone numbers from innocent civilians who happened to be in the area when the stingray was activated.

Like the overbroad hard drive seizure in *Ganias*, the overbroad seizure of hundreds of phone numbers of innocent people is a necessary component of this investigative technique. One response to this problem would be to simply ban the technique altogether—the seizure of so much information is not worth the benefit to law enforcement. But a more nuanced approach would be to impose a use restriction on the information that is recovered. For example, only the suspect's cell phone number (once identified) can be used, and all the other cell phone numbers must be permanently deleted. This was the approach of a district court judge in a recent case. The judge authorized the use of the stingray only if the government agreed not to use the "innocent" phone numbers for any purpose, explaining that "[m]inimizing procedures such as the destruction of private information the United States has no right to keep are necessary to protect the goals of the Fourth Amendment."[188]

F. Drones and Police Body Cameras

The growing use of surveillance drones by law enforcement brings up another type of challenge to Fourth Amendment doctrine. Drones are a specific example of the new technologies that law enforcement officers can use as a force multiplier, allowing one officer to conduct the same amount of surveillance that would have required five, ten, or even more officers in the past.[189] Drones are

185. *Id.* at 5.

186. *Id.*

187. Presumably the law enforcement officers already have the appropriate level of suspicion with regard to the defendant to justify their application for a pen/trap or a wiretap.

188. *See In re* the Application of the U.S. for an Order Relating to Tels. Used by Suppressed, No. 15 M 0021, 2015 WL 6871289 at *10 (N.D. Ill. Nov. 9, 2015).

189. Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 606 (2017).

used to patrol the international border,[190] monitor traffic patterns,[191] take photos of crime scenes,[192] search for missing persons,[193] and even to watch for escaping defendants during police raids.[194] So far, their use in active criminal investigations has been rare,[195] but their potential application in crime detection as mobile surveillance devices is obvious. Not only can drones carry powerful cameras that can view activity from a significant distance, they can also be equipped with high-resolution microphones or even stingrays that intercept cell phone metadata or content.[196] Some of these surveillance options, such as thermal imagers that monitor private residences, would constitute a search at the collection stage,[197] but others, such as cameras in public places,[198] do not implicate the Fourth Amendment.

Like the GPS tracking at issue in *Jones* or the private closed-circuit television cameras present in innumerable public places,[199] widespread law enforcement use of surveillance drones could provide

190. Paul McBride, *Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations*, 74 J. AIR L. & COM. 627, 635 (2009) (describing a Predator drone that flew along the United States-Mexico border and helped to capture over 2,000 undocumented aliens and over 8,000 pounds of marijuana over a seven-month period); *but see* Craig Whitlock, *U.S. Surveillance Drones Largely Ineffective Along Border, Report Says*, WASH. POST (Jan. 6, 2015), https://www.washingtonpost.com/world/national-security/us-surveillance-drones-largely-ineffective-along-border-report-says/2015/01/06/5243abea-95bc-11e4-aabd-d0b93ff613d5_story.html [https://perma.cc/X8ZV-GEU7] (reporting that less than two percent of the nearly 121,000 illegal border crossers were apprehended with the help of drones).

191. See Morrison, *supra* note 27, at 753.

192. Chris Francecsani, *Domestic Drones are Already Reshaping U.S. Crime-Fighting*, REUTERS (Mar. 3, 2013), http://www.reuters.com/article/2013/03/03/us-usa-drones-lawenforcement-idUSBRE92208W20130303 [https://perma.cc/PY6L-98VZ] (describing a deputy sheriff who uses a drone to take photographs at crime scenes from multiple altitudes, in order to "bring the crime scene right into the jury box").

193. *Id.* (describing a private drone pilot who worked with police and helped to locate ten missing persons during search and rescue operations).

194. Jason Koebler, *Court Upholds Domestic Drone Use in Arrest of American Citizen*, U.S. NEWS (Aug. 2, 2012), http://www.usnews.com/news/articles/2012/08/02/court-upholds-domestic-drone-use-in-arrest-of-american-citizen [https://perma.cc/VZD3-W3JA].

195. Morrison, *supra* note 27, at 753–54.

196. *Id.* at 752–53.

197. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

198. United States v. Houston, 813 F.3d 282, 287–90 (6th Cir. 2016). Indeed, even ten weeks' worth of camera surveillance of a suspect's front was not considered a "search" by the Sixth Circuit.

199. There are an estimated thirty million surveillance cameras in the United States, though this number includes private and public surveillance cameras. Suzanne Choney, *Lawmakers Want More Surveillance on the Ground—and in the Sky*, NBC NEWS (Apr. 20, 2013), http://usnews.nbcnews.com/_news/2013/04/20/17830619-lawmakers-want-more-surveillance-on-the-ground-and-in-the-sky?lite [https://perma.cc/KL3C-RDBH].

enormous gains for deterring and investigating criminal activity.[200] It could also provide the government with enormous amounts of information about individuals without the need to prove any individualized suspicion. One possible way to avoid these privacy intrusions would be to restrict the ways in which law enforcement officers can use drones to collect information. For example, a legislature could pass a law stating that the police can only use a drone for a criminal investigation if the police had reasonable suspicion or probable cause. Such a limitation could come directly from the courts as well, but as with the mosaic theory, this would require a significant restructuring of Fourth Amendment doctrine regarding reasonable expectations of privacy in public places.

So far states and the federal government have been reluctant to place limitations on law enforcement use of drones,[201] perhaps because legislatures are concerned about denying the police access to this powerful new tool in a time when there is increased worry about terrorist activity.[202] Once again, use restrictions on the data could be a solution to this problem. Law enforcement drones could be allowed to surveil public places by the thousands, recording and storing huge amounts of information, but police could only access the information upon a showing of probable cause, reasonable suspicion, or at least a demonstration that the information is likely relevant to an ongoing criminal investigation.[203] To take an obvious example, if a crime occurs in public at a certain time and a certain place, law enforcement officers would be authorized to access the databank of drone records

200. Studies have shown that installing CCTV cameras leads to a significant decrease in crime, especially when the cameras are installed in parking lots and public transportation. Brandon C. Welsh & David P. Farrington, *Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis*, 26 JUST. Q. 716, 732–33 (2009).

201. In contrast, many states have passed laws limiting the private use of drones for data collection. For an overview of state laws in the civil privacy context, see Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1158–62 (2015). For example, Texas has passed a law banning the use of drones to capture images with the "intent to conduct surveillance." *Id.* at 1159; TEX. GOV'T CODE ANN. § 423.003 (West, Westlaw through 2017 Reg. Sess.).

202. For example, public surveillance cameras were instrumental in tracking down and identifying the Boston Marathon bombers. Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 23 (2013). Drones could be even more useful than stationary cameras in many such situations.

203. This last phrase mirrors the language in the Pen/Trap statute, which law enforcement officers must comply with when they seek to obtain non-content information about a communication. The Pen/Trap statute requires that officers certify that "the information likely to be obtained is relevant to an ongoing criminal investigation . . . ." 18 U.S.C. § 3122(b)(2) (2012).

to see whether a drone had observed and recorded any aspect of the crime with these time and place restrictions as limitations. As another example, once a person becomes suspected of a crime, police officers would be authorized to use their drone database to review that person's movements over the past few weeks and perhaps dedicate a drone to their movements in the near future. This would be another example of the "ongoing seizure" type of use restriction.

Professor Stephen Henderson proposes a similar use restriction regime in the context of police body cameras.[204] Calling police body cameras "government time machines," Professor Henderson argues that recording everything that every police officer sees promises significant benefits, such as preserving evidence that might otherwise be lost, mischaracterized, or forgotten by the witnesses,[205] as well as deterring and exposing improper police conduct.[206] But since these body cameras also record a large amount of innocent, private activity, Professor Henderson proposes use restrictions on the video that is recorded, including "security from unauthorized access, need-to-know limitations, audit logs, and destruction schedules."[207] These restrictions could come from police administrative rules, legislative action, or even by an aggressive interpretation of the Fourth Amendment. As Professor Henderson argues, "[r]eturning to the home after completion of the search would of course require a new warrant," so reviewing and perhaps even enhancing a video recording of the initial search of the home should also be viewed as its own separate search.[208]

Professor Henderson acknowledges the limits of use restrictions; indeed, he argues that use restrictions should usually only be used to supplement more traditional restrictions on "front-end" data

204. *See* Henderson, *supra* note 149, at 960–71.
205. *Id.* at 966–68.
206. *Id.* at 968–70.
207. *Id.* at 970.

> [G]iven the myriad benefits of tamper-resistant, always-on officer recording, it seems such recording is worth the privacy cost. But this merely means police should record. It remains to be determined—or should remain to be determined—what can be done with those recordings .... Thus, as an administrative matter in police department guidelines, as a legislative matter, and—I would argue—as a matter of Fourth Amendment (and state constitutional analog) reasonableness, there should be use and disclosure limitations on that data.

Id.

208. *Id.* at 970–71.

collection.[209] But in the case of police body cameras, he notes that they would only record views that an officer is lawfully entitled to see; thus, body camera images are already subject to a "built-in" front-end data collection restriction.[210]

The analogy between police body cameras and drones is not a perfect one. While it is true that in both cases the law enforcement action is subject to *some* level of front-end collection restriction, the rules regarding what a police officer can do (and where she can go) during a criminal investigation are detailed and well established. In contrast, the only rules regarding what a drone can do and where it can go is the public place/private place distinction, and even that distinction provides scant protection in light of the "flyover" cases that allow law enforcement officers in planes and helicopters to observe even the curtilage of a home.[211] Furthermore, police body cameras do no more than record what a human police officer is already seeing; thus, they do not gather any more information than the officer does with his own eyes. Drones, on the other hand, can allow the police to increase their surveillance power a hundredfold or more at far less cost.[212] Thus, the historic economic check on government surveillance is much less effective.[213]

But the analogy remains useful. Both drones and police body cameras represent technologies that allow for significant increase in detecting and deterring crime, and this increase rises exponentially if the data collection restrictions are kept to a minimum. If drones are only allowed to operate after reasonable suspicion or probable cause has been established, they will be unable to deter and detect unforeseen criminal activity. Police body cameras that can only gather data at the discretion of the police officer or the suspect will likewise fail to provide a useful record of either police abuse or potential criminal activity.[214] Thus, the best solution in both situations could be

209. *Id.* at 962. Professor Henderson has his own significant critiques of use restrictions, which is discussed in Part V.

210. *Id.* at 963.

211. California v. Ciraolo, 476 U.S. 207, 212–15 (1986).

212. *See* Levinson-Waldman, *supra* note 189, at 606.

213. Judges have been wary of surveillance technology that allows law enforcement to leverage its surveillance power. *See, e.g.*, United States v. Jones, 565 U.S. 400, 418–31 (2012) (Alito, J., concurring) (arguing that courts must step in to protect the public from continuous GPS surveillance because the traditional practical limits on surveillance no longer applied). I have critiqued this point of view as overly simplistic. *See* Ric Simmons, *Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment*, 36 HARV. J.L. & PUB. POL'Y 550, 557–79 (2013).

214. Professor Henderson acknowledges this as well, noting that "there might be circumstances when it is impossible to get the desired law enforcement safety benefit

to allow for relatively unlimited data collection,[215] but to merely record and store the data unless and until the government can show a specific need for it.

G. *Creating Binary Searches*

A "binary search" is a search that only reveals the presence or absence of illegal activity, such as a field test for narcotics or a drug-sniffing dog. The Supreme Court has held that this type of surveillance is not a Fourth Amendment search, since it only reveals private information to the police if illegal activity is occurring, and individuals have no legitimate expectation of privacy in illegal activity.[216] In one sense, the binary search doctrine is merely a type of use restriction, since it states that if a certain kind of data can only be used to prove criminal activity, then collecting that data is not a Fourth Amendment search.

By the same token, use restrictions can theoretically be used to turn many types of surveillance into a binary search. Machines could gather information about a suspect, but not share this information with any human being. Software would then process this information into a binary result: either there is probable cause to believe the suspect has committed a crime, or there is not. If there is no probable cause of criminal activity, the data would never be shared with anyone, and (theoretically) the suspect's Fourth Amendment rights would not have been implicated.[217] If there is probable cause of criminal activity, the machine would notify the law enforcement officer, and the officer would obtain a warrant to access the data. This is an example of the "future use" version of use restrictions, since it is the future use of the data that determines whether collecting the data itself is constitutional—if the data is only "seen" by machines, then the Fourth Amendment does not apply.[218]

---

without completely abandoning front-end acquisition restraints, as with broad scale, panvasive drone surveillance, or with broad scale, panvasive Internet surveillance for malware." Henderson, *supra* note 149, at 960. This Article discusses the application of use restrictions for Internet surveillance in Section III.A.1.

215. Unlimited, that is, within the contours of existing Fourth Amendment and legislative rules.

216. *See* United States v. Place, 462 U.S. 696, 707 (1983) (stating in dicta that using a drug-trained dog is not a "search" because it can only reveal information of illegal activity, in which the defendant has no legitimate expectation of privacy); *see also* Illinois v. Caballes, 543 U.S. 405, 409–10 (2005) (same).

217. *See* Covey, *supra* note 28, at 1312–16.

218. Orin Kerr has a somewhat different interpretation of binary searches, or at least of the field test that the Court approved of in *United States v. Jacobsen*, 466 U.S. 109 (1984). He applies "ongoing seizure" doctrine to that case, noting that in *Jacobsen* the

These technology-based binary searches could take many forms. Companies have already developed portable "gun detectors" that measure the radiation emitted by a person's body and can tell whether the radiation is being blocked by a firearm.[219] If the law enforcement officer using the gun detector sees an actual image of all the items being carried by an individual, using the device would likely be a search under the Fourth Amendment since it would be revealing information in which the suspect has a reasonable explanation of privacy.[220] But assume the device does not display any images to its user. Instead, the device uses software to examine the image and determine whether one of the items carried by the suspect was a gun, and if it determines that a gun was present, it would emit a noise or cause a light to flash. If the device were used in a context in which it was illegal to carry a firearm,[221] this process would transform a Fourth Amendment search into a binary search since the law enforcement

---

agents lawfully seized the defendant's package of cocaine, and then destroyed a trace amount of that substance when they conducted a field test. Kerr, *supra* note 9, at 20–24 (citing *Jacobsen*, 466 U.S. at 111–12). The Court noted in dicta that if the government had destroyed a large portion of the substance in their field test, the intrusion into the suspect's privacy interests would have been greater and thus the seizure may have been unreasonable. *Jacobsen*, 466 U.S. at 125. Kerr used this dicta as evidence that government actions *after* a seizure has been made can transform a reasonable, constitutional search into an unreasonable, and thus unconstitutional, search. Kerr, *supra* note 9, at 20–24. This application of *Jacobsen* provides only weak support for the adoption of use restrictions because it requires us to view the government actions in *Jacobsen* as one ongoing seizure which could be made illegal at any point if the government "misuses" the item that is seized. It makes more sense, however, to view *Jacobsen* as two distinct seizures—first, the package is seized (which is reasonable for a short period of time) and second, a portion of the substance is destroyed in the test (which is reasonable if the size of the portion is *de minimis*). If the second seizure is unreasonable because too much of the substance is destroyed, that makes the *second* seizure illegal, but it does not mean that the *first* seizure now also becomes illegal—unless you choose (as Kerr does) to conflate the government actions into one ongoing seizure.

219. *See, e.g.*, John Rudolph, *NYPD Testing Long-Distance Gun Detection Device*, HUFFPOST (Jan. 18, 2012), http://www.huffingtonpost.com/2012/01/18/nypd-gun-detection-device_n_1213813.html [https://perma.cc/JNV3-9R4T].

220. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the government's use of a thermal imaging-device to detect the heat emerging from inside a house was a "search" under the Fourth Amendment).

221. For example, in a jurisdiction where concealed carry is not permitted, or in a jurisdiction which allows for concealed carry, but requires any individual who interacts with a police officer to inform him or her that she is carrying a firearm. *See, e.g.*, OHIO REV. CODE ANN. § 2923.126(A) (West, Westlaw through 2017 File 23 of 132d Gen. Assemb. (2017–2018) & 2017 State Issue 1) ("If a licensee is stopped for a law enforcement purpose and if the licensee is carrying a concealed handgun at the time the officer approaches, the licensee shall promptly inform any law enforcement officer who approaches the licensee while stopped that the licensee has been issued a concealed handgun license and that the licensee currently is carrying a concealed handgun ....").

officer using the device would learn nothing private about the suspect unless the suspect were carrying an illegal item.

Similarly, if the government installed software on internet service providers to monitor the internet traffic passing from one computer to another and sent all of the information to be reviewed by a law enforcement officer, courts would almost certainly consider that to be a search under the Fourth Amendment.[222] But if the government instead installed a more sophisticated piece of software that autonomously analyzed each piece of data flowing past and only notified law enforcement if a known piece of child pornography was in transit, the government agents would learn nothing about the suspects' data unless the suspect was engaged in criminal activity.[223] In each of these examples, the government is *collecting* the data, but the collection is not deemed a search because of the way the data is *used* after it is collected: it is only given to machines to process, not to human beings.[224]

H. Solving the Encryption Dilemma

Law enforcement officers are facing a serious and growing problem with the ever-increasing sophistication of encryption

222. There is an argument that under the third-party doctrine, such monitoring would not be a "search" because every individual who uses an internet service provider is knowingly sharing all of the information with a third party. *See, e.g.*, United States v. Miller, 425 U.S. 435, 440–43 (1976) (holding that a bank depositor does not have a reasonable expectation of privacy in any information he has knowingly turned over to his bank). This argument is not likely to survive in the current digital age. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 285–88 (6th Cir. 2010) (holding that an individual has a reasonable expectation of privacy in the emails that are sent through a third-party internet service provider).

223. For a more detailed discussion of these advanced types of binary searches, see Ric Simmons, *The Two Unanswered Questions of* Illinois v. Caballes: *How to Make the World Safe for Binary Searches*, 80 TUL. L. REV. 411 (2005).

224. This use of the binary search doctrine could be combined with the mosaic theory discussed earlier. *See supra* Section II.A. It is certainly possible that the government could develop algorithms sophisticated enough to determine probable cause of illegal activity from dozens or even hundreds of seemingly innocuous facts about a subject. Thus, even if courts adopt a "data processing" type of use restriction and determine that the processing of massive amounts of public data could be considered a search, courts could also then apply a "future use" type of use restriction and determine that the processing is not a search if the mechanical processor does not turn the results over to human law enforcement officers unless there is clear evidence of criminal activity. This would require a very sophisticated algorithm, one that is capable of not only determining the likelihood of criminal activity, but also determining whether that likelihood rises to the level of probable cause. In the context of detecting hidden guns or digital files of child pornography, it is pretty clear when criminal activity is present; in the context of the massive amounts of information processed under a mosaic theory doctrine, the determination will be much more difficult.

technology. As digital devices become more secure, law enforcement officers are occasionally unable to access the information on those devices, even if they are legally entitled to do so by a valid court order. In two recent cases,[225] the FBI sought to force Apple to decrypt information on devices that the company had built. In each case, the FBI had the right to the information under the Fourth Amendment, but was initially unable to access the information due to the strength of the encryption.[226]

This tension between the need to have secure devices and the need for law enforcement to gain access when they are legally authorized to do so is only going to increase as hyper-encrypted devices become more and more common. In order to ensure that the government is able to access these devices when they have a court order, law enforcement officers are asking Congress to pass legislation requiring manufacturers to build "backdoors" into all of their encryption software.[227] For example, Congress could require all manufacturers of encrypted devices to provide a key to their encryption and place that key in escrow, available to the government only if the appropriate legal standards are met.[228] Under this model, the government will collect and hold the keys to millions of digital devices, but will be forbidden from using any key unless it obtained a court order.[229] This could be seen as a "data processing" form of use restriction—the actual search occurs not when the government automatically collects all of the passwords, but when it uses the passwords to process the encrypted material and extract the information. However, this solution would give law enforcement the power to break into any encrypted software, a power that would be limited only by the legal restrictions created by the courts and the

225. *See In re* Apple, Inc., 149 F. Supp. 3d 341, 345 (E.D.N.Y. 2016); *In re* the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016).

226. 149 F. Supp. 3d at 345; 2016 WL 618401, at *1.

227. Spencer Ackerman, *FBI Chief Wants "Backdoor Access" to Encrypted Communications to Fight ISIS,"* GUARDIAN (July 8, 2015), https://www.theguardian.com/technology/2015/jul/08/fbi-chief-backdoor-access-encryption-isis [https://perma.cc/5NCW-HXHG].

228. This idea has been floated before in a different context, when some members of Congress proposed that all telephones and computers had to be equipped with a "Clipper Chip," which would provide the users with the highest level of encryption technology, but would give the government backdoor decryption keys. *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 743, 752, 755–57 (1995).

229. *See id.*

legislatures. As noted below,[230] it may be unwise to give that much information access to law enforcement officials.

III. ARGUMENTS AGAINST USE RESTRICTIONS

As we have seen, use restrictions offer potential solutions to some of the more difficult Fourth Amendment problems that courts are facing today. However, these solutions come with doctrinal challenges and strong policy implications.

A. Doctrinal and Political Obstacles

As noted in Part I, there are three ways that use restrictions can be given legal authority: appellate courts could adopt use restrictions as one of the factors in deciding whether government surveillance violates the Fourth Amendment; magistrates and lower court judges could write use restrictions into their search warrants; and/or legislatures could create use restrictions through statute. However, the first and third method face considerable practical challenges. Courts have so far shown little appetite for adopting use restrictions, and altering Fourth Amendment jurisprudence to accommodate use restrictions carries its own set of problems. On the other hand, if legislatures create use restrictions, there is no need to worry about maintaining a coherent legal doctrine, but there will be a considerable amount of political resistance to overcome.

1. Use Restrictions in Case Law

For decades, the Supreme Court has focused on the collection of data in its Fourth Amendment jurisprudence, and the Court has shown no signs that it is willing to change its focus. As noted above, the Court has refused to adopt use restrictions in areas where they would make the most sense, including the mosaic theory,[231] DNA databanks,[232] and, with a few limited exceptions, special needs searches.[233]

---

230. *See* Section III.B.2.

231. *See supra* Section II.A. *See generally* United States v. Jones, 132 S. Ct. 945 (2014) (applying a trespass analysis when deciding whether attaching a GPS device to a car and monitoring the car's movements for four weeks qualified as a search, while the plurality suggested a mosaic theory, but none of the Justices proposed use restrictions).

232. *See supra* Section II.B; *see also* Maryland v. King, 133 S. Ct. 1958, 1962 (2013) (allowing law enforcement to take DNA samples from felony arrestees).

233. *See supra* Section II.C; *see also* Mich. Dep't of State Police v. Sitz, 494 U.S. 444, 450–51 (1990) (allowing suspicionless police roadblocks to check for drunk drivers); *contra* Bd. of Educ. v. Earls, 536 U.S. 822, 829 (2002) (suggesting that the way the government uses the data is a factor in determining whether the collection of the data is constitutional);

To be fair, we have seen growing numbers of lower courts turning to use restrictions to solve some of the modern problems posed by technology and the Fourth Amendment: the Ninth Circuit used a sequester type of use restriction when granting a warrant for searching a computer;[234] the Second Circuit applied an ongoing seizure use restriction to the seizure and search of a hard drive;[235] and a District Court in Illinois imposed a use restriction on the collection of phone numbers with a stingray device.[236] So it is possible that some forms of use restriction will ultimately be adopted by the Supreme Court.

But even if the Supreme Court were willing to reorient its Fourth Amendment jurisprudence to include use restrictions, a serious doctrinal ambiguity would have to be resolved. It is relatively easy to determine when the government collects evidence; even in the digital age, it is obvious when the government takes possession of information. Thus, it is relatively easy to create rules that restrict when the government is allowed to collect information. But what, exactly, constitutes a "use" of information? And at what point does any specific use transform the government action into a Fourth Amendment search?

These line-drawing questions are evident in some versions of the data-processing model of use restrictions. Adopting these use restrictions could be a useful way of evaluating government conduct in the context of the mosaic theory, DNA databases, or encrypted digital devices. In the latter two instances, courts can set out relatively clear rules about which uses are permitted and which are not: testing the DNA for any purpose other than to determine identity would constitute a search, and using a password to open a digital device would also constitute a search. But what types of data processing constitute a forbidden use in the context of the mosaic theory?

Ferguson v. City of Charleston, 532 U.S. 67, 79–81 (2001); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 665 (1995); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 626 n.7 (1989).

234. *See supra* notes 165–168 and accompanying text; *see also* United States v. Comprehensive Drug Testing, 579 F.3d 989, 1003 (9th Cir. 2009) (en banc) (inserting a use restriction into the search warrant).

235. *See supra* notes 174–183 and accompanying text; *see also* United States v. Ganias, 755 F.3d 125, 137 (2d Cir. 2014) (restricting the use of digital data once it was in the possession of law enforcement).

236. *See supra* text accompanying note 188; *see also In re* Application of the U.S. for an Order Relating to Tels. Used by Suppressed, No. 15-M-0021, 2015 WL 6871289, at *10 (N.D. Ill. Nov. 9, 2015).

One answer would be for a court to hold that data processing constitutes a search when the information it reveals infringes on the suspect's reasonable expectation of privacy.[237] But this will require a whole new set of case law to explore what type of information violates a person's reasonable expectation of privacy and what does not. For example, assume that under a use restrictions regime, the government is allowed to collect and store all of our telephone and email metadata—that is, it can keep a record of everyone we have called or emailed over the past five years—but it cannot process this data if the result of the data processing violates a reasonable expectation of privacy. Checking the metadata of one phone call will not violate this use restriction, since determining the name of one person called does not infringe on a reasonable expectation of privacy, at least as currently defined by the Supreme Court.[238] But beyond that easy case, courts will very quickly get embroiled in some very challenging line-drawing questions. What if the government throws tens of thousands of emails and telephone calls into an algorithm and learns that a suspect called a therapist ten times in one year? Or what if an analysis shows that at one point the defendant called a criminal defense attorney six times in a forty-eight-hour period? Or it could be that the analysis turns up nothing remotely embarrassing or incriminating, but still gives police an outline of the suspect's communications pattern: 23% of his phone calls were to his spouse; 32% were to colleagues at work; 5% were to college friends who live out of town, and so on. At what point does the level of detail infringe on an individual's reasonable expectation of privacy? More importantly, how would the law enforcement agent who is conducting the analysis know ahead of time whether the results would be so personal that it would violate the suspect's reasonable expectation of privacy?

Another possible answer would be for courts to hold that certain types of data processing automatically violate a suspect's reasonable expectation of privacy, regardless of what the results of the processing might be. So, for instance, courts could determine that law enforcement officers conduct a Fourth Amendment search any time

237. *See, e.g.*, Logan, *supra* note 21, at 1605–06; Laurie Buchan Serafino, *"I Know My Rights, So You Go'n Need a Warrant for That": The Fourth Amendment,* Riley*'s Impact, and Warrantless Searches of Third-Party Clouds*, 19 BERKELEY J. CRIM. L. 154, 176, 181–84 (2014) (arguing that a government inspection of data constitutes a search).

238. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979). Although *Smith* is much maligned for its broad application of the third-party doctrine, its address/content distinction has never been seriously challenged in the courts. Thus, address information remains unprotected by the Fourth Amendment.

they use at least ten days' worth of location information from a cell phone, or the metadata of a hundred different telephone calls, or more than a thousand purchases on a credit card. These rules may be an improvement on the current regime that focuses on the collection of the data, but they will inevitably be arbitrary.

It will also be challenging to define the scope of permissible uses for the future use restrictions that we see in the context of special needs searches and binary searches. There are thousands of different ways the government could use information that it collects, and courts will need to rule on each of them to see if they fit into the special needs category or the binary search category. In the special needs context, courts will have to decide whether the government's use of the information is far enough removed from a law enforcement purpose to make the search permissible.[239] Some uses will be directly related to a law enforcement purpose, such as using the results of a breathalyzer in a prosecution for drunk driving, while others may be more ambiguous, such as studying the driving patterns of self-driving cars to learn if the car is being parked in an illegal parking spot. In the binary search context, courts will have to decide how certain the result of the machine's analysis needs to be before the results can be turned over to a law enforcement officer. Some machines may reveal with near absolute certainty that criminal activity is occurring, such as a gun detector that is 99.9% accurate and is used in a location where firearms are prohibited, while others may only show a mere probability that criminal activity is occurring, such as an analysis of key words used in emails that are sent to known criminal associates.

In short, although use restrictions can help courts bypass some tricky doctrinal issues with regard to collection restrictions and new technology, they also create their own set of tricky doctrinal issues that require resolution. This once again leads us to consider imposing use restrictions through legislatures since legislatures have the freedom to regulate law enforcement surveillance creatively, without any need to tie the regulation to the language of the Fourth Amendment or conform to a consistent jurisprudence. Unfortunately, legislatures are more responsive to political pressures than courts, and use restrictions could be a hard sell in many contexts.

239. As noted above in Section II.C., in theory, courts only approve of special needs searches if they are conducted for a purpose other than law enforcement. *See, e.g.*, Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 633–34 (1989) (allowing suspicionless drug testing of railroad employees in order to ensure the safety of railway passengers).

2. Statutory Use Restrictions

Legislatures have already adopted use restrictions in some criminal law contexts. For example, the Foreign Intelligence Service Act ("FISA") sets out specific rules for conducting electronic surveillance for foreign intelligence purposes.[240] These rules are different from (and arguably more lenient than) the rules for conducting electronic surveillance for criminal law purposes.[241] FISA incorporates use restrictions in two ways: first, the agent seeking a FISA order must certify that a "significant purpose of the surveillance is to obtain foreign intelligence information,"[242] which is an example of a future use restriction; and second, the information cannot be used in a routine criminal case unless a court certifies that the information was lawfully obtained and the surveillance conformed with a court order, which is an example of a very weak form of sequestering restriction.[243]

The government also applies a sequestering version of a use restriction in its tax collection system: in order to encourage complete disclosure of income for tax purposes, the Internal Revenue Service ("IRS") keeps all tax returns confidential, and will not share them with the immigration authorities to assist in identifying illegal aliens or with the FBI to assist in criminal investigations.[244]

Thus, there are precedents to setting up statutory use restrictions for policy reasons. In the FISA context, Congress has determined that the enhanced need for information in the foreign intelligence context requires a different standard for obtaining that information,[245] while in the IRS context, Congress believes that sequestering tax information will encourage widespread and honest reporting of income.[246] This is similar to the motivation for many proposals for use

240. *See, e.g.*, 50 U.S.C. §§ 1801(f), 1804(a) (2015).

241. Essentially, the FISA requirements provide a lower legal standard but require a higher level of administrative approval than similar provisions under the Electronic Communications Privacy Act. *See How the NSA's Surveillance Procedures Threaten America's Privacy*, ACLU, https://www.aclu.org/fact-sheet/documents-confirm-how-nsas-surveillance-procedures-threaten-americans-privacy [https://perma.cc/NM7V-LBLC].

242. *See* 50 U.S.C. § 1804(a).

243. *See id.* § 1806(g).

244. *See* I.R.C. § 6103 (2015); *see also* Kerr, *supra* note 8, at 7 ("The basic idea is that the government is a 'they' not an 'it,' and limiting data sharing is essentially the same as limiting data collection for individual groups and institutions with different roles within the government.").

245. *See* 50 U.S.C. §§ 1801–1811.

246. *See Disclosure Laws*, IRS (last modified Oct. 15, 2015), https://www.irs.gov/government-entities/federal-state-local-governments/disclosure-laws [https://perma.cc/XH6Y-

restrictions in the criminal law context. For example, in the national security context, Congress might decide that a particular risk is so severe (such as the hijacking of an airplane) or a particular danger is so immediate (such as an imminent terrorist attack) that the usual collection restrictions on law enforcement should not apply.[247] In the broader context of special needs searches, the government might seek information for a regulatory, non-criminal purpose, such as the movement patterns of self-driving cars. Allowing the collection for a national security or regulatory purpose but forbidding its use for law enforcement purposes could make the initial collection of the data more reasonable.

Unfortunately, these use restrictions are likely to be politically unpopular, both among law enforcement officials and among the general public. This would especially be true in the national security context. Imagine the public reaction if the government identified a potential terrorist and obtained incriminating evidence about him, but then took no criminal action.[248] Even in less dramatic cases, such as drunk driving checkpoints or body camera footage, it may be hard to convince the public of the wisdom of use restrictions. If the government has evidence of criminal activity and yet does not arrest or prosecute the perpetrator, it is likely that political pressure will be brought to bear to weaken or even eliminate the use restrictions.

B. Policy Problems

The second critique of use restrictions is more substantive than political unpopularity. Although use restrictions promise to solve a number of challenging modern search and seizure issues, they create their own set of problems. First, widespread adoption of use restrictions may have the unintended consequence of weakening collection restrictions, or at least slowing the momentum to reforming

---

GBVC] (clarifying that the IRS cannot disclose tax information to law enforcement officers without a court order); *see also* I.R.C. § 61013(j).

247. Of course, generally legislatures cannot weaken protections that are based on the Fourth Amendment, so they would be unable to replace Fourth Amendment collection restrictions with weaker, statutory-based use restrictions in the national security context. But courts have been relatively deferential to legislatures in matters regarding foreign intelligence and national security, so legislatures have more leeway in designing the proper mix of collection restrictions and use restrictions in the national security context. *See, e.g.*, United States v. Davis, 482 F.2d 893, 910 (9th Cir. 1973) (allowing suspicionless searches at airports because of the enormous danger to lives and property and because hijackings involve a "serious risk of complications in our foreign relations").

248. *See, e.g.*, Christopher Slobogin, *Government Dragnets*, 73 LAW & CONTEMP. PROBS. 107, 130 n.145 (2010) ("[A] prohibition on prosecuting terrorists who are caught in an antiterrorist program would be very hard for the public to swallow.").

or broadening collection restrictions. Second, the mere fact that our personal data is being collected and stored, even if there are legal protections against it being used without court approval, could be seen as overly invasive. And finally, on the other side of the argument, aggressive adoption of use restrictions might go too far in hampering law enforcement's job in detecting and preventing crime.

1. The Law of Unintended Consequences: Use Limitations Would Discourage Restrictions on Data Collection

Today, all Americans have their search queries and credit card charges monitored, processed, and packaged by corporations;[249] the recipients and lengths of their phone calls catalogued;[250] their movements through public spaces recorded.[251] Some of this monitoring is done by the government; most of it is done by private companies (who often turn over the information to the government upon request).[252] This trend shows every sign of increasing, with the growing prevalence of smart devices, cloud storage, and other methods by which private companies collect and store our information.[253]

But the pervasive private and public surveillance of the modern world is not just different in degree—it is different in kind. The in-person surveillance of past generations tended to overwhelmingly focus on the poor and on ethnic minorities.[254] This arguably resulted in an underdeveloped legal opposition to government surveillance. If the critical dilemma of surveillance law is how to balance privacy with security, all too often this involved balancing one group's privacy with another group's security. But now that is changing. The machines and private companies that are assisting the government in building the modern surveillance state engage in a much broader-based, even-

249. Henderson, *supra* note 25, at 704.

250. *Id.* at 704, 707.

251. *Id.* at 704–05.

252. *Id.* at 704–07; Amitai Etzioni, *A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach*, 10 I/S J.L. & POL'Y FOR INFO. SOC'Y 641, 665 (2014).

253. Henderson, *supra* note 25, at 705–06.

254. *See, e.g.*, Tracey Maclin, *Race and the Fourth Amendment*, 51 VAND. L. REV. 333, 333 (1998) ("[P]olice targeting of black people for excessive and disproportionate search and seizure is a practice older than the Republic itself."); Morrison, *supra* note 27, at 761 ("For migrants, minorities and the urban poor, universal visual surveillance would not necessarily take away their privacy; they have already lost it."); William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1267 (1999) ("[P]eople who have money have more Fourth Amendment protection than people who don't.").

handed surveillance.[255] This will have—indeed, already is having—a profound effect on popular attitudes about how much privacy people are willing to cede to private companies and to law enforcement.[256]

Now that enfranchised classes are being subjected to heightened levels of surveillance, the political impetus to create stricter limitations on information gathering is growing.[257] In other words, a more uniform distribution of privacy infringement will naturally lead to political pushback against this increased surveillance.[258] Even the courts may be more responsive to Fourth Amendment claims when the surveillance affects every citizen.[259]

As we saw in the previous section, use restrictions may be one way that this pushback occurs. When faced with the dilemma of protecting privacy in the face of overwhelming levels of private and

255. *See* Morrison, *supra* note 27, at 762–64. Of course, modern surveillance techniques may not result in a broader range of society being subject to surveillance. Many critiques of big data are based on the concern that the machines and algorithms use data that is already tainted by pre-existing bias in the criminal justice system. *See, e.g.*, ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING 131–32 (2017) ("Police data remains colored by explicit and implicit bias.").

256. The revelations of the NSA's mass surveillance program led to widespread protests and ultimately culminated in a revision of the USA PATRIOT Act that limited the authority of the NSA. *See* Heather Kelly, *Protests Against the NSA Spring Up Across U.S.*, CNN (July 5, 2013, 7:24 AM), http://www.cnn.com/2013/07/04/tech/web/restore-nsa-protests/ [https://perma.cc/7UTA-PN95]; *see also* USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 269 (2015) (codified in scattered sections of U.S.C.).

257. Writing in the context of ubiquitous drone surveillance, Professor Morrison notes:

> If everyone were equally surveilled, it might achieve what Randall Kennedy suggested some years ago: rather than burdening particular individuals with a "racial tax," universal surveillance would increase taxes across the board. It is the same argument that can be made in favor of police checkpoints—everyone is a little bit inconvenienced so that a few don't have to be singled out and bear the burden for everyone else.
>
> In this sense, domestic drone surveillance's greatest social and intellectual contribution might not only be that it might help revitalize a generalized impetus to protect privacy interests. It may also make us think more directly about the uses and abuses of government power, a reality with which some of us—though arguably few of those who write about these topics—are already intimately familiar.

Morrison, *supra* note 27, at 761–62.

258. Henderson, *supra* note 20, at 555–59.

259. During the oral argument of *United States v. Jones*, Chief Justice Roberts asked the government's attorney whether he believed it would be a search if the government put a GPS device on the cars of all the Supreme Court Justices and monitored all their movements for a month. The government attorney answered in the affirmative. *See* Transcript of Oral Argument at 9–10, United States v. Jones, 565 U.S. 400 (2012) (No. 10-1259). The Court ultimately found against the government in a surprisingly unanimous decision. *Jones*, 565 U.S. at 401.

government data collection, courts and legislatures may abandon efforts to control or regulate the surveillance itself and instead limit government use of the information. Although this reaction may increase citizens' privacy rights in the short term, in the long term it will almost certainly decrease the pressure on courts and legislatures to craft meaningful restrictions on data collection.[260] The result could be a loosening of the restrictions on data collection, allowing the government greater access to Americans' personal information than ever.[261] Thus, the public will become more accustomed to mass collection of data, and more tolerant of greater intrusions into our private lives.

Current law already allows for mass collection of data in a number of contexts. Surveillance cameras can constantly monitor public places without any legal restrictions at all, and each one can scan thousands or tens of thousands of people in a short period of time. These cameras could use facial recognition software to identify people with outstanding arrest warrants;[262] they could also track who is associating with whom in order to build a profile of a person's activity that could ultimately lead to a probable cause determination. As noted above, current law allows for the collection of DNA

260. Some supporters of use restrictions see the loosening of collection restrictions as an important step in ensuring that use restrictions are effective:

> The best way to achieve the benefits of computer surveillance while minimizing the privacy risks is to place greater focus on the later regulatory stages, and in particular, the final stage of public disclosure. If computer surveillance is likely to be effective, genuinely achieving a significant public good, widespread collection and analysis is necessary to achieve those benefits. The law should respond by adding new protections to the output end of the regulatory stage: The law should allow the collection and manipulation of data, but then place significant limits on the use and disclosure of the information.

Kerr, *supra* note 8, at 8.

261. Professor Christopher Slobogin makes this argument in the special needs context:

> Freed from any [collection] restrictions on its antiterrorism efforts, the executive branch might introduce numerous such programs, believing that, at the least, bombs will be discovered and terrorists identified.... [T]his approach allows the government to carry out other suspicionless "special needs" searches and seizures as long as evidence thereby obtained is not used in a criminal court. Thus school students can be suspended, illegal immigrants deported through a civil process, and house residents subjected to civil fines based on dragnet stops and searches without violating the Fourth Amendment, despite the thousands of innocent individuals affected by drug testing, checkpoints, and health and safety inspections, respectively.

Slobogin, *supra* note 248, at 130 n.145.

262. *See* John J. Brogan, *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, 25 HASTINGS COMM. & ENT. L.J. 65, 80–81 (2002).

samples from arrestees[263] and the tracking of (at least some) movements on public roads.[264] More broadly, the third-party doctrine theoretically allows the government to access enormous amounts of information, such as telephony metadata, credit card purchases, digital information stored in the cloud, or search engine requests.

There is, however, a growing sense that these doctrines need to be reformed in the modern era in response the powerful data collecting tools that are now available to law enforcement. One need look no further than the two most recent Supreme Court cases that dealt with technology and the Fourth Amendment. In *United States v. Jones*, four concurring Justices adopted the mosaic theory and said that there should be a limit on the government's ability to collect information about a person's movements in public,[265] while a fifth Justice called into question the entire third-party doctrine.[266] In *Riley v. California*, all nine Justices held that cell phones contain such a large amount of information that they are immune from the search incident to lawful arrest exception to the warrant requirement.[267]

Widespread adoption of use restrictions could blunt or even halt this call for reform. If the courts create strong barriers in how the government is permitted to use this information, they will face less pressure to limit the collection of this information. If the information that the government obtained is limited at the use stage, why bother to untangle the thicket of the third-party doctrine just to protect information that can only be used if it belongs to criminals? Likewise, why try to solve all the difficult problems posed by the mosaic theory if we can protect citizens at the back end of the investigation instead? The same benefits and simplicity of use restrictions that make them attractive will also likely lead courts to rely on them exclusively in these challenging cases.

In time, we may begin to see use restrictions that not only *supplement* the current regime of collection restrictions, but that begin to *replace* the current regime of collection restrictions. For example, assume that the government develops a binary-search gun detector like the one described in a previous Section,[268] that can detect the presence of a concealed firearm and then sends a message

263. *See supra* text accompanying notes 80–81.

264. *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983) (allowing the government to monitor the movement of a car during one trip over public roads).

265. United States v. Jones, 565 U.S. 400, 429–31 (2012) (Alito, J., concurring).

266. *Id.* at 254 (Sotomayor, J., concurring).

267. Riley v. California, 134 S. Ct. 2473, 2484–85 (2014).

268. *Supra* Section II.G.

to the user only if a firearm is present. This detector would be quite effective if the government were able to use it indiscriminately in any context in which concealed firearms are illegal. But courts would only permit this kind of indiscriminate use if they held that machine observation alone does not constitute a search. This in itself is a controversial claim—a court could easily hold that a "search" is occurring when a government-controlled machine obtains information.[269] But assuming the courts adopt such a position, the implications are somewhat troubling. If the government cannot look at the information without a warrant, courts may be persuaded to allow the government to collect and store all sorts of data information stored on our cell phones or computers, the content of our telephone conversations or emails; all of this could potentially be collected by machines under the theory that human beings will never see it unless there is evidence of criminal activity.

2. Panvasive Surveillance and the Panopticon—The Consequences of Allowing the Government to Collect and Store the Data

The second problem with use restrictions is that they may not truly protect our privacy in any meaningful way. The mere collection and storage of data infringes on our privacy by creating a chilling effect on our activities. Meanwhile, rogue government officials could abuse their positions by violating use restrictions, for either professional or personal reasons. And finally, use restrictions may not last forever—a doctrinal shift by courts or a political shift in the legislatures could mean that all of the information that the government has collected and stored would no longer be protected.

Privacy law experts are divided about how effective use restrictions can be in protecting our privacy.[270] Use restrictions are relatively popular tools in the civil privacy realm, under the theory that much of the harm from a loss of privacy comes from the way the

269. At least one commentator has argued that "information disclosed only to an automated system remains 'private' as that word is commonly used and as it is used in Fourth Amendment law." Matthew Tokson, *Automation and the Fourth Amendment,* 96 IOWA L. REV. 581, 611–12 (2011). This would be consistent with current case law. For example, the Supreme Court has held that a government-controlled dog that sniffs the defendant's property does not constitute a Fourth Amendment search (even though the dog itself learns many private things about the suspect when she conducts the sniff) because the human handler learns nothing other than the presence or absence of contraband. Illinois v. Caballes, 543 U.S. 405, 409–10 (2005). By analogy, a machine (whether it is a gun detector or a software sniffer) that "learns" a lot of private information about a suspect is not conducting a search because the human learns nothing other than the presence or absence of contraband.

270. Thanks to Craig Konnoth for helping me to navigate through this debate.

once-private information is used once it is obtained.[271] Private information can be used to steal someone's identity, discriminate against a person based on race or religion, or damage a person's reputation.[272] We also count on having exclusive use of our private information to control how we interact with the general public, our professional colleagues, and our most intimate friends.[273] And finally, controlling the use of our own information allows us freedom to adopt idiosyncratic or counter-majoritarian beliefs or attitudes without risk of societal or legal repercussions.[274]

All of these concerns are arguably assuaged by a robust application of use restrictions. If an individual can know with complete confidence that use restrictions would ensure that her private information would not be shared or misused, she would be agnostic as to whether it was collected or stored. This argument has moved many privacy experts away from collection restrictions and towards use restrictions. President Obama's Council of Advisors on Science and Technology released a report which argued that "[p]olicy attention should focus more on the actual uses of big data and less on its collection and analysis."[275]

But some privacy scholars disagree. In one of the seminal works on privacy, Professor Daniel Solove provides a taxonomy of privacy violations, which lists four categories of violations: information collection, information processing, information dissemination, and invasion.[276] Use restrictions can only protect an individual against the second and third category of privacy violations; as Professor Solove argues: "Even if no information is revealed publicly, information

271. *See* Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. NAT'L SEC. L. & POL'Y 333, 335–37 (2014).

272. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT 78 (Stanford Univ. Press ed., 2010).

273. *See, e.g.*, FERDINAND DAVID SHOEMAN, *Privacy and Intimate Information*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 403, 406 (Ferdinand David Shoeman ed., 1984); Charles Fried, *Privacy*, 77 YALE L.J. 475, 476–83 (1968).

274. *See* Nissenbaum, *supra* note 2722, at 82.

275. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., EXEC. OFFICE OF THE PRESIDENT, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/8YC2-9BFP]. Policymakers have also moved to alter Fair Information Practice Principles towards use restrictions and away from collection restrictions. *See* Fred H. Cate, Peter Cullen, & Victor Mayer-Schönberger, *Data Protection Principles for the 21st Century Revising the 1980 OECD Guidelines*, OXFORD INTERNET INST. (Mar. 2014), http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf [https://perma.cc/W2AA-MTA3].

276. Daniel J. Solove, *A Taxonomy of Privacy*, 145 U. PA. L. REV. 477, 490 (2006).

collection can create harm."[277] Professor Solove focuses on the discomfort that individuals generally feel when they know they are being monitored, as well as the chilling effect that will deter them from saying or doing unconventional things.[278] To be fair, individuals may feel less of this discomfort or chilling effect if they are only being monitored by machines, but even under the most strict and limited use restriction regime, individuals would know that it was possible that the information that was being collected could be seen and used by a human being.

And of course most use restriction regimes do not promise that *nobody* will see the information; only that its disclosure will be limited to certain people and/or to fulfill certain purposes.[279] Many versions of use restrictions merely bar law enforcement from using the information in a criminal prosecution; this does not mean that law enforcement officers cannot ever have access to it.[280] For example, law enforcement officers may be permitted to use the data to determine which individuals are persons of interest, so that they can focus resources on those people. And even if there is a strict sequestration from all law enforcement personnel, many of the proposed use restrictions would allow *some* member of the government to see the information, perhaps for regulatory purposes. This would undoubtedly have a chilling effect on an individual's statements and actions.[281]

As noted above,[282] the Supreme Court seems to agree with the proposition that the mere collection of information, regardless of how or whether it is used, can be a violation of privacy. In *Planned Parenthood v. Casey*,[283] the Supreme Court noted that its precedents

277. *Id.* at 491.

278. *Id.* at 499 (footnote omitted) ("[P]ublic surveillance can have chilling effects that make people less likely to associate with certain groups, attend rallies, or speak at meetings. Espousing radical beliefs and doing unconventional things takes tremendous courage; the attentive gaze, especially the government's, can make these acts seem all the more daring and their potential risks all the more inhibitory.").

279. For example, the "sequestration" model of use restrictions would allow certain law enforcement agencies to have access to the information; likewise, the "future use" model would, by definition, allow the government to use the information for certain approved purposes. *See supra* Sections I.A.4, I.A.5.

280. See for example the use restriction imposed by the warrant in *United States v. Ganias*, 755 F.3d 125, 139 (2d Cir. 2014), *vacated*, 791 F.3d 290 (2015) (mem.); *see also supra* notes 174–83 and accompanying text.

281. *See* Henderson, *supra* note 149, at 962 ("[K]nowing that all of our movements, online or off, will be recorded for potential observation can very meaningfully chill those actions.").

282. *Supra* Section III.B.1.

283. 505 U.S. 833 (1992).

have acknowledged a "private realm of family life which the state cannot enter."[284] And in the criminal law context, the Supreme Court recently recognized this problem in *Birchfield v. North Dakota*,[285] a case in which the Court struck down state laws that imposed criminal penalties if a driver suspected of drunk driving refused to take a blood test.[286] In contrasting blood tests to breath tests, the Court noted that the blood sample from blood alcohol tests can be preserved by the state, and that the state could conduct further tests to learn intimate information about the suspect.[287] Even if use restrictions were put into place to forbid the government from conducting any further tests of the suspect's blood, "the potential [for such tests] remains and may result in anxiety for the person tested."[288]

This leads to the second, related problem with relying upon use restrictions: none of them will be foolproof. Once the information is stored in government databases, individual government officials could conceivably gain access to it, even if such access is unauthorized under law. A rogue government official could use the information for professional purposes, such as to help guide a criminal investigation, or for personal purposes, such as to learn information about an ex-spouse, neighbor, or friend.[289] Often, unauthorized access would take place in secret and neither the victim nor other government employees would even know that it occurred—but everyone would know at the collection stage that the potential for such disclosure existed. Even if the misuse is not intentional, officials in charge of the information could mistakenly allow it to end up in the wrong hands.[290]

---

284. *Id.* at 851 (quoting Prince v. Massachusetts, 321 U.S. 158, 166 (1944)).

285. 136 S. Ct. 2160 (2016).

286. *Id.* at 2178.

287. *Id.*

288. *Id.*

289. For example, in *United States v. Czubinski*, an IRS employee routinely accessed confidential IRS databases without authorization. 106 F.3d 1069, 1071–72 (1997). He looked up tax returns of his political opponents, his girlfriend, a prosecutor who had investigated his father, and many other social acquaintances. *Id.*

290. A useful analogy can be made with medical information, which is strictly protected by the Health Insurance Portability and Accountability Act ("HIPAA"). A recent investigation by ProPublica revealed that the Department of Veteran's Affairs alone was responsible for more than 10,000 privacy violations between 2011 and 2015. *See* Annie Waldman & Charles Ornstein, *Privacy Violations Rising At Veterans Affairs Medical Facilities*, NAT'L PUB. RADIO (Dec. 30, 2015), http://www.npr.org/sections/health-shots/2015/12/30/461400692/patient-privacy-isn-t-safeguarded-at-veterans-medical-facilities [https://perma.cc/32T3-UJY5]. A recent article in the Berkeley Medical Journal noted that

> [although] some violations of HIPAA are maliciously willful, much leakage of private information is accidental. The wide range of communications available to parties throughout various healthcare entities exposes significant risks. Familiar

The government's information databases would also be vulnerable to private parties who could illegally gain access to the data, observe it, and then disclose it or use it for their own purposes. Cyberattacks on credit card companies, retail stores, and banks are relatively common in today's world;[291] there is no way to ensure that the massive amounts of data being collected and stored by the government for future use would be immune from such intrusions.[292]

Finally, there is always the danger that government policy will change and that use restrictions will be weakened or eliminated. At that point, law enforcement will have an enormous amount of information that was essentially collected under false pretenses—under a promise that it would never be used by the police. Arguably, the larger the database grows, the more pressure the government will be under to loosen the use restrictions so that the government can use the information to achieve its goals. It is not hard to imagine a dramatic event—a terrorist attack, a sharp increase in crime, a credible threat of danger—that could push policymakers to change the laws.

All of these concerns translate into a significant and justified political resistance to the widespread collection of our private information. The American public would likely not feel comfortable if the government had a complete DNA database of every citizen, even if the government could not access the database without a

---

> sources of information leakage may include exposed documents on desks, uncollected output from fax machines and printers, improperly disposed documents, or a lost laptop or USB memory card or stick. With the popularity of social networking, the potential for HIPAA violations is magnified through personal blogs of healthcare workers or information posted in Facebook or other social networking sites. Even an activity as mundane as discussing in public areas information regarding a patient may represent a significant source of information leakage.

Lauren Mock, *When Patient Health Information Leaks*, ISSUES BERKELEY MED. J. (2012), https://issues.berkeley.edu/articles/20.1_Mock_L_Patient_Health_Information_Leaks_HIPAA.html [https://perma.cc/JG2M-9XGX]. The same concerns would exist for any government-held private information, regardless of how many legal protections are put into place.

291. *See* Jim Finkle & Mark Hosenball, *Exclusive: More Well-Known U.S. Retailers Victims of Cyber Attacks*, REUTERS (Jan. 11, 2014), http://www.reuters.com/article/us-target-databreach-retailers-idUSBREA0B01720140112 [https://perma.cc/W2VB-ELRY]; John O'Donnell & Alexander Winning, *Banks Reinforce Cyber Defences After Global Attack*, REUTERS (May 15, 2017), http://www.reuters.com/article/cyber-banks-idUSL2N1IH1K6 [https://perma.cc/EZF6-UAZJ].

292. *See* Paul McLaughlin, *Crypto Wars 2.0: Why Listening to Apple on Encryption Will Make America More Secure*, 30 TEMP. INT'L & COMP. L.J. 353, 380 (2016).

warrant.[293] Similarly, the government would encounter strong resistance if it sought the password into the backdoor of every digital device that we owned, even if it would be legally prohibited from using the password without a court order.

In short, a regime in which use restrictions replace collection restrictions will carry serious risks to our privacy. And yet many use restrictions (such as those on binary searches, or those involving the mosaic theory) are only effective if they *replace* front-end collection restrictions so that the government can access the data when permitted to do so.

3. Limiting Law Enforcement

The final critique of use restrictions comes from the other end of the political spectrum: they may unduly hamper law enforcement efforts to detect and prevent crime. This critique can be applied to attempts to impose use restrictions on previously unregulated surveillance, such as collecting telephone metadata, tracking public activities, recording activity with police body cameras, or obtaining information from third parties. In all of these areas, law enforcement officials are eager to use new technologies to further their criminal investigations, and use restrictions will discourage or even prevent such use. As noted above,[294] barring this evidence from criminal cases will likely make these use restrictions politically unpalatable, but it would also arguably be bad policy.

This Article has already discussed the policy problems that would arise if the courts imposed use restrictions in the special needs context.[295] On the one hand, use restrictions would be an effective way to bypass the disingenuous nature of many of the Court's special needs cases. Courts have approved drug testing in schools,[296] drunk driving checkpoints,[297] or searches at airports[298] based on the dubious premise that these searches serve needs unrelated to law enforcement. Use restrictions could turn this legal fiction into reality, by ensuring that any information obtained by law enforcement can only be used for the non-law enforcement purpose (protecting a conducive learning environment, keeping roadways safe, preventing

293. *See* Arnold H. Loewy, *A Proposal for the Universal Collection of DNA*, 48 TEX. TECH L. REV. 261, 262–63 (2015).

294. *See supra* text accompanying note 248.

295. *See supra* Sections III.B.1, III.B.2.

296. New Jersey v. T.L.O., 469 U.S. 325, 347–48 (1985).

297. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

298. *See, e.g.*, United States v. Davis, 482 F.2d 893, 898 (9th Cir. 1973).

terrorism) and not used in criminal proceedings against the suspect. But imposing use restrictions would potentially mean that individuals who sell drugs in school, drive while intoxicated, or attempt to bring firearms or explosives onto airplanes would all be immune from prosecution. Thus, although it may appear unjust to some people, it will also weaken the deterrence value of the work done by law enforcement officers.

Police officer body cameras are another example of how use restrictions could unduly impede law enforcement duties. There is currently a robust debate about how to handle the massive amount of video footage being compiled by body cameras.[299] Many advocates have raised concerns about the privacy rights of the individuals—innocent and guilty—who are caught on camera.[300] Much of what police officers see—and which is captured by their body cameras—is private information, taking place inside someone's home, or involving verbal descriptions of intimate or potentially embarrassing situations.[301] Thus, there are privacy concerns if the general public is able to view this information indiscriminately, and use restrictions can be imposed to prevent public dissemination.

Some commentators have registered concern with using body camera footage in criminal investigations, even though existing front-end collection restrictions already ensure that the footage is inadmissible if the recording officer was violating the Fourth Amendment. As Professor Stephen Henderson has pointed out:

> [H]igh quality cameras would record all sorts of events and details never noticed by the officers, and potentially permanently store them for later high-tech perusal (e.g., zoom in and slow down). Moreover, for things an officer does notice . . . the digital record will remain forever pristine, whereas memories quickly degrade and even fade entirely.[302]

---

299. *See, e.g.*, McKenzie Funk, *Should We See Everything a Cop Sees?* N.Y. TIMES MAG. (Oct. 18, 2016), https://www.nytimes.com/2016/10/23/magazine/police-body-cameras.html [https://perma.cc/4LES-WT76 (dark archive)].

300. *See, e.g.*, Jay Stanley, *Police Body-Mounted Cameras: With Right Policies In Place, A Win for ALL*, ACLU (Mar. 2015), https://www.aclu.org/other/police-body-mounted-cameras-right-policies-place-win-all [https://perma.cc/9K58-HQVD].

301. *See* Henderson, *supra* note 149, at 964 ("Such cameras would record not 'only' events taking place in public, but instead would record everywhere officers go, including the interiors of our homes and therefore potentially under every bed and into every dresser.").

302. *Id.* (footnotes omitted). Professor Henderson also recommends "security from unauthorized access, need-to-know limitations, audit logs, and destructions schedules." *Id.* at 970.

Thus, body cameras do more than just record what an officer is already allowed to see under the Fourth Amendment; the cameras act as sort of an observer-on-steroids—seeing everything, forgetting nothing. Under this view, body cameras are an overly invasive type of investigation that is not sufficiently covered by collection restrictions. Once again, use restrictions seem like an elegant solution to this problem: record everything, even the most intimate details that may have been unnoticed by the officer herself, but restrict access to the footage by requiring the police to show probable cause or obtain a warrant before viewing the footage.[303]

But imposing such a restriction would severely blunt the strong potential that body cameras have to assist law enforcement officers in investigating crimes. A warrant requirement would not be so onerous when the prosecutor wanted to obtain footage of the defendant actually committing the crime for which he is currently being charged—in such cases, probable cause would be easy to establish and the video footage would provide an excellent source of evidence for the jury. But for long-term investigations, law enforcement officers may need to review over hundreds of hours of footage, to spot patterns in behavior or take note of facts that may not have been obvious to the officer who was wearing the camera. The very features that arguably make body cameras overly intrusive—the ability to capture minute details and preserve those details forever—make them invaluable to police investigators who are pursuing these investigations. Requiring a warrant before allowing police access to this data would seriously hamper these legitimate efforts.

Yet another example can be found in applying use restrictions to the third party doctrine. As with the rules governing binary searches, the third party doctrine represents a jurisprudence which initially made sense when it was developed in an earlier era, but which has transformed into a doctrine which allows law enforcement officers access to the millions of pieces of data that we all share with private companies. The potential privacy intrusions created by the third party doctrine have only been exacerbated in recent years as the government has improved its data processing abilities. Use restrictions appear to provide a solution to this dilemma: allow law enforcement officers access to this data, thus keeping the third-party doctrine intact, but force them to obtain a warrant—or some kind of court authorization—before they can process the data to detect patterns and learn intimate facts about the suspect.

303. *Id.* at 970–71.

Privacy advocates would no doubt cheer such a development, but law enforcement officers will correctly point out that such a rule would create an odd dissonance between the rights of law enforcement and the rights of private commercial entities. Private companies, the very entities who are collecting this information, can buy, sell, and process this data with impunity. They do so in order to maximize their profits, by marketing products to us with greater precision, engaging in price discrimination, and developing new products that they believe we will purchase.[304] Creating use restrictions for law enforcement officers will mean that companies will be able to use this information to further their own profit-seeking goals, while law enforcement officers will not be able to use the information in order to engage in legitimate crime control.

Of course, on one level this dissonance is nothing new: private parties have never been subject to the Fourth Amendment and so they have always faced fewer *constitutional* restrictions than law enforcement officers. But for the most part private parties face some kind of legal restrictions that are equal to or even greater than those imposed on law enforcement. Private parties are not allowed to trespass on our private property, search our clothes or our belongings, hack into our computers, or eavesdrop on our telephone conversations. As the recent plurality decision in *United States v. Jones* pointed out, Fourth Amendment restrictions have historically been tied to notions of common law trespass.[305] If anything, government agents have had more power to intrude on our privacy than private parties: law enforcement agents can search through open fields;[306] detain us and frisk us if they have reasonable suspicion of a crime;[307] and (unlike private parties) obtain court orders to enter our homes or wiretap our phones without our consent.[308] It would thus be anomalous to give private companies unlimited power to process and use the data they collect, but to prohibit the government from doing so unless they obtained permission from a court.[309]

304. *See, e.g.*, Henderson, *supra* note 25, at 706 (describing how "Target's analytics department managed to piece together when a customer is pregnant ... because such a significant life event shakes up our otherwise routine habits.").

305. 565 U.S. 400, 405 (2012).

306. Oliver v. United States, 466 U.S. 170, 184 (1984).

307. Terry v. Ohio, 392 U.S. 1, 30–31 (1968).

308. *See* 18 U.S.C. § 2518 (2012) (allowing the government to wiretap phones if they receive the appropriate court order).

309. One response to this critique, of course, would be to impose similar use restrictions on how private companies can process or use our data, thus putting private companies and law enforcement on similar footing. Another response would be to point out that it is appropriate to put greater restrictions on the government than on private

CONCLUSION

For all their promise and potential, use restrictions are deeply problematic. The Supreme Court has consistently refused to incorporate them into its Fourth Amendment jurisprudence, even in cases in which they would provide a solution to the problem at hand. Legislatures will find them politically challenging to enact: those on the left will argue that they will supplant or discourage robust collection restrictions, and thus will result the government collecting and storing massive amounts of our intimate data; those on the right will protest the fact that information that proves criminal activity (or could, with proper data mining, lead to such proof), is kept out of the hands of law enforcement. And from a policy standpoint, use restrictions could impede the development of more robust collection restrictions, while allowing the government to collect and store massive amounts of data that would be vulnerable to misuse in a variety of ways.

But the term "use restrictions" is quite broad, encompassing many different types of surveillance regulation. These different types of use restrictions vary in degrees of scope, effect, and legal authority; thus, one-size-fits all proposals or critiques are not particularly useful. In particular, there is one type of modest use restriction that has a sound legal basis, is relatively easy to implement, and does not carry the same danger as most of the other: the use restrictions that are written into warrants by magistrates or trial judges. This type of use restriction presents no doctrinal difficulties: judicial officers have always had the power to limit the scope of warrants that they issue, and so restricting the information obtained through a warrant (either the sequester model or the ongoing seizure model) does not require any reevaluation of Fourth Amendment jurisprudence. These use restrictions can be applied on a case-by-case basis in any situation in which the government needs to apply for a warrant, such as to search digital devices or using stingrays or other surveillance tools to intercept electronic communication. Eventually, appellate courts could even write these limitations into law, arguing that these necessarily overbroad searches are only constitutional if they are

---

parties because the government has much greater power over individuals; unlike private companies, the government has the coercive power of the state. However, the criminal justice system responds to this power imbalance by creating limitations on the use of this state power—for example, the Fourth Amendment requires government agents to obtain a warrant before conducting most searches, *see* United States v. Ventresca, 380 U.S. 102, 106 (1965), and requires reasonable suspicion before government agents can seize an individual, *see* Terry v. Ohio, 392 U.S. 1, 30–31 (1968).

accompanied by the appropriate use restriction. This will also create uniformity among the different lower court judges, providing them with guidance as to when such use restrictions are required and how they should be structured.

But until the practical and legal problems with use restrictions can be resolved, courts and legislatures should resist adopting use restrictions in any other context. Law enforcement officers will routinely offer to submit to use restrictions in exchange for the ability to engage in overbroad searches, such as collecting DNA information, conducting searches for national security purposes, and obtaining third party information. At this point, courts and legislatures should confine use restrictions to a case-by-case basis in individual warrants, and focus instead on reforming the rules on collection restrictions in order to deal with the growing challenges created by new surveillance technologies.

We know that law enforcement officers, for legitimate reasons, have an insatiable appetite for collecting information, and modern tools for amassing and processing data will only increase this appetite. At first, use restrictions appear to be a reasonable way of navigating this new world: if the drive to collect information is unstoppable, and the current Fourth Amendment restrictions on collecting the information are outdated or insufficient, then it appears logical to give up on the collection stage and protect our rights at the stage where it seems to matter the most—when the information is actually being observed by a law enforcement official or used against us in court. But in reality, most use restrictions promise more than they can deliver.